华为 HCIA 认证备考宝典
完备的配套习题，夯实内容理解

异步图书
www.epubit.com

华为HCIA路由交换认证指南

韩立刚　薛中伟　宋晓锋　郑汉钦　著



中国工信出版集团　人民邮电出版社
POSTS & TELECOM PRESS

目　　录

版权信息

版 权

内容提要

前 言

致 谢

资源与支持

第1章 认识计算机网络

1.1 Internet的产生和中国的ISP

1.1.1 Internet的产生和发展

1.1.2 中国的ISP

1.1.3 跨运营商访问网络带来的问题

1.1.4 多层级的ISP结构

1.2 局域网的发展

1.2.1 局域网和广域网

1.2.2 同轴电缆组建的局域网

1.2.3 集线器组建的局域网
1.2.4 网桥优化以太网
1.2.5 网桥MAC地址表构建过程
1.2.6 交换机组网
1.2.7 以太网网卡
1.3 企业局域网的规划和设计
1.3.1 二层结构的局域网
1.3.2 三层结构的局域网
1.4 通信领域常见的术语
1.4.1 速率
1.4.2 带宽
1.4.3 吞吐量
1.4.4 时延
1.4.5 时延带宽积
1.4.6 往返时间
1.4.7 利用率
1.5 传输媒体
1.5.1 导向传输媒体
1.5.2 非导向传输媒体
1.6 网络分类
1.6.1 按网络的范围进行分类

1.6.2 按网络的使用者进行分类
1.7 习题

第2章 TCP/IP
2.1 介绍TCP/IP
2.1.1 理解协议
2.1.2 TCP/IPv4栈的分层
2.1.3 TCP/IPv4栈各层的功能
2.1.4 封装和解封
2.2 应用层协议
2.2.1 应用和应用层协议
2.2.2 应用层协议的标准化
2.2.3 以HTTP为例认识应用层协议
2.2.4 抓包分析应用层协议
2.2.5 应用层协议和高级防火墙
2.3 传输层协议
2.3.1 TCP和UDP的应用场景
2.3.2 TCP首部
2.3.3 TCP连接管理
2.3.4 TCP可靠传输的实现
2.3.5 UDP
2.3.6 传输层协议和应用层协议之间的关系

2.3.7 服务和端口之间的关系
2.3.8 端口和网络安全的关系
2.4 网络层协议
2.4.1 网络层协议的两个版本
2.4.2 IPv4
2.4.3 ICMP
2.4.4 ARP
2.4.5 IGMP
2.5 数据链路层协议
2.6 物理层协议
2.7 OSI参考模型和TCP/IP
2.8 习题

第3章 IP地址和子网划分
3.1 学习IP地址预备知识
3.1.1 二进制和十进制
3.1.2 二进制数的规律
3.2 理解IP地址
3.2.1 MAC地址和IP地址
3.2.2 IP地址的组成
3.2.3 IP地址格式
3.2.4 子网掩码的作用

3.2.5 子网掩码的另一种表示方法
3.3 IP地址详解
3.3.1 IP地址分类
3.3.2 特殊的IP地址
3.4 私网地址和公网地址
3.4.1 公网地址
3.4.2 私网地址
3.5 子网划分
3.5.1 为什么需要子网划分
3.5.2 等长子网划分
3.5.3 等长子网划分示例
3.5.4 变长子网划分
3.5.5 点到点网络的子网掩码
3.5.6 判断IP地址所属的网段
3.5.7 子网划分需要注意的几个问题
3.6 合并网段
3.6.1 合并网段的方法
3.6.2 合并网段的规律
3.6.3 判断一个网段是超网还是子网
3.7 习题
第4章 管理华为设备

4.1 介绍华为网络设备操作系统
4.2 eNSP简介
4.2.1 安装eNSP
4.2.2 华为设备型号
4.3 VRP命令行
4.3.1 命令行的基本概念
4.3.2 命令行的使用方法
4.4 登录设备
4.4.1 用户界面配置
4.4.2 通过Console口登录设备
4.4.3 通过Telnet登录设备
4.4.4 通过SSH登录设备
4.5 基本配置
4.5.1 配置设备名称
4.5.2 配置设备时钟
4.5.3 配置设备IP地址
4.6 配置文件的管理
4.6.1 华为设备配置文件
4.6.2 保存当前配置
4.6.3 设置下一次启动加载的配置文件
4.6.4 文件管理

4.6.5 将配置导出到FTP或TFTP服务器
4.7 习题
第5章 静态路由
5.1 路由基础
5.1.1 什么是路由
5.1.2 路由信息的来源
5.1.3 路由优先级
5.1.4 网络畅通的条件
5.1.5 配置静态路由示例
5.1.6 浮动静态路由
5.2 路由汇总
5.2.1 通过路由汇总精简路由表
5.2.2 路由汇总例外
5.2.3 无类域间路由（CIDR）
5.3 默认路由
5.3.1 全球最大的网段
5.3.2 使用默认路由作为指向Internet的路由
5.3.3 使用默认路由和路由汇总简化路由表
5.3.4 默认路由造成路由环路
5.3.5 让默认路由代替大多数网段的路由
5.3.6 Windows上的默认路由和网关

5.4 网络排错案例

5.4.1 站在全局的高度排除网络故障

5.4.2 计算机网关也很重要

5.5 习题

第6章 动态路由

6.1 什么是动态路由

6.2 动态路由——OSPF协议

6.2.1 OSPF协议简介

6.2.2 由最短路径生成路由表

6.2.3 OSPF协议相关术语

6.2.4 OSPF工作过程

6.2.5 OSPF报文类型

6.2.6 OSPF三张表

6.2.7 OSPF区域

6.3 配置OSPF协议

6.3.1 OSPF多区域配置

6.3.2 查看OSPF协议的3张表

6.3.3 在区域边界路由器上进行路由汇总

6.3.4 OSPF协议配置排错

6.4 虚拟路由冗余协议（VRRP）

6.5 习题

第7章 交换机组网
7.1 交换机常规配置
7.2 交换机端口安全
7.2.1 交换机端口安全详解
7.2.2 配置交换机端口安全
7.2.3 镜像端口监控网络流量
7.3 生成树协议
7.3.1 交换机组网环路问题
7.3.2 生成树协议概述
7.3.3 生成树协议基本概念和工作原理
7.3.4 生成树的端口状态
7.3.5 STP的缺点和RSTP概述
7.3.6 查看和配置STP
7.4 VLAN
7.4.1 什么是VLAN
7.4.2 理解VLAN
7.4.3 跨交换机VLAN
7.4.4 链路类型和端口类型
7.4.5 VLAN的类型
7.4.6 配置基于端口的VLAN
7.4.7 配置基于MAC地址的VLAN

7.5 实现VLAN间通信
7.5.1 使用多臂路由器实现VLAN间路由
7.5.2 使用单臂路由器实现VLAN间路由
7.5.3 使用三层交换实现VLAN间路由
7.6 端口隔离
7.7 链路聚合
7.7.1 链路聚合的基本概念
7.7.2 链路聚合技术的使用场景
7.7.3 链路聚合的模式
7.7.4 链路聚合配置示例
7.8 习题
第8章 网络安全
8.1 ACL简介
8.1.1 ACL的组成
8.1.2 ACL设计思路
8.2 使用基本ACL实现网络安全
8.2.1 使用基本ACL实现内网安全
8.2.2 使用基本ACL保护路由器安全
8.3 使用高级ACL实现网络安全
8.4 AAA
8.4.1 AAA工作方式

8.4.2 AAA的配置
8.5 习题
第9章 网络地址转换和端口映射
9.1 公网地址和私网地址
9.2 NAT的类型
9.2.1 静态NAT
9.2.2 动态NAT
9.2.3 网络地址端口转换（NAPT）
9.2.4 Easy IP
9.3 静态NAT的实现
9.4 NAPT的实现
9.5 Easy IP的实现
9.6 配置端口映射
9.7 灵活运用NAPT
9.7.1 “悄悄”在公司网络中接入一个网段
9.7.2 实现单向访问
9.8 习题
第10章 将路由器配置为DHCP服务器
10.1 静态地址和动态地址
10.2 将华为路由器配置为DHCP服务器

10.3 跨网段分配IP地址

10.4 使用接口地址池为直连网段分配地址

10.5 习题

第11章 IPv6

11.1 IPv6的优势

11.1.1 IPv6的基本首部

11.1.2 IPv6的扩展首部

11.2 IPv6地址

11.2.1 IPv6地址格式

11.2.2 IPv6地址分类

11.2.3 单播地址

11.2.4 组播地址

11.2.5 任播地址

11.2.6 常见的IPv6地址类型和范围

11.3 IPv6地址配置

11.3.1 计算机和路由器的IPv6地址

11.3.2 IPv6单播地址业务流程

11.3.3 邻居发现协议

11.3.4 IPv6地址配置方式

11.3.5 IPv6地址自动配置的两种方式

11.4 实现IPv6地址自动配置

11.4.1 实现IPv6地址无状态自动配置
11.4.2 抓包分析RA和RS数据包
11.4.3 实现IPv6地址有状态自动配置
11.5 IPv6路由
11.5.1 IPv6静态路由
11.5.2 OSPFv3
11.6 习题

第12章 广域网
12.1 广域网
12.2 PPP介绍
12.2.1 PPP原理
12.2.2 PPP基本工作流程
12.3 配置PPP
12.3.1 配置PPP：身份验证用PAP 模式
12.3.2 配置PPP：身份验证用CHAP模式
12.3.3 抓包分析PPP链路建立过程
12.3.4 配置PPP为另一端分配地址
12.4 PPPoE
12.4.1 PPPoE概述
12.4.2 PPPoE报文格式
12.4.3 PPPoE的工作过程

12.4.4 配置Windows PPPoE拨号上网
12.4.5 配置路由器PPPoE拨号上网
12.5 习题

第13章 VPN
13.1 虚拟专用网络
13.1.1 专用网络
13.1.2 虚拟专用网络
13.2 配置站点间VPN
13.2.1 GRE隧道VPN
13.2.2 介绍IPSec VPN
13.2.3 配置IPSec VPN
13.2.4 基于Tunnel接口的IPSec VPN
13.3 远程访问VPN
13.4 习题

第14章 WLAN技术
14.1 WLAN概述
14.1.1 什么是WLAN
14.1.2 WLAN标准和Wi-Fi世代
14.1.3 Wi-Fi在办公场景的发展趋势
14.2 WLAN基本概念和产品

14.2.1 WLAN设备介绍
14.2.2 基本的WLAN组网架构
14.2.3 敏捷分布式AP架构
14.2.4 有线侧组网概念
14.2.5 无线侧组网概念
14.3 WLAN的工作原理
14.3.1 WLAN工作流程
14.3.2 第一阶段：AP上线
14.3.3 第二阶段：WLAN业务配置下发
14.3.4 第三阶段：STA接入
14.3.5 第四阶段：WLAN业务数据转发
14.4 案例：旁挂二层组网隧道转发
14.4.1 配置网络互通
14.4.2 配置AP上线
14.4.3 配置WLAN业务参数
14.5 习题
第15章 园区网典型组网案例
15.1 企业情况介绍
15.1.1 物理拓扑
15.1.2 组网要求
15.2 网络规划和配置

15.2.1 网络设备部署

15.2.2 VLAN规划和子网划分

15.2.3 创建VLAN配置干道链路

15.2.4 指定生成树的根交换机

15.2.5 配置VLAN间路由

15.2.6 配置静态路由

15.2.7 将汇聚层交换机配置成DHCP

15.2.8 配置WLAN

15.2.9 配置到WLAN网络的路由

15.2.10 配置网络地址转换和端口映射

15.2.11 创建ACL实现内网上网控制

15.2.12 配置VPN

版权信息

书名：华为HCIA路由交换认证指南

ISBN：978-7-115-57173-1

本书由人民邮电出版社发行数字版。版权所有，侵权必究。

您购买的人民邮电出版社电子书仅供您个人使用，未经授权，不得以任何方式复制和传播本书内容。

我们愿意相信读者具有这样的良知和觉悟，与我们共同保护知识产权。

如果购买者有侵权行为，我们可能对该用户实施包括但不限于关闭该帐号等维权措施，并可能追究法律责任。

版　　权

著　　韩立刚　薛中伟　宋晓锋　郑汉钦

责任编辑　武晓燕

人民邮电出版社出版发行　　北京市丰台区成寿寺路11号

邮编　100164　　电子邮件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

读者服务热线：(010)81055410

反盗版热线：(010)81055315

内容提要

本书是针对HCIA最新考试大纲编写的认证教材。全书共分为15章，首先介绍了计算机网络的产生和演进、计算机通信使用的协议、IP地址和子网划分等内容；然后介绍了使用华为设备进行企业组网的基本技术，包括路由器和交换机的基本配置、IP地址的规划、静态路由和动态路由的配置、使用交换机进行组网等内容；最后讲解了高级网络技术，其中涉及网络安全的实现、网络地址转换和端口映射、将路由器配置为DHCP服务器以实现IP地址的自动分配，以及IPv6、广域网、VPN、无线局域网等相关知识；第15章园区网典型组网案例将企业组网的技术进行了综合运用。

本书以理论知识为铺垫，重点凸显内容的实用性，旨在通过以练代学的方式提升读者的理论水平和实操能力。本书除了适合备考华为HCIA认证的人员阅读，还适合有志于投身于网络技术领域的新人阅读，也适合开设了网络专业课程的高校师生阅读。

前　　言

我大学学的是无机化工，1999年毕业后到化肥厂上班，直觉告诉我IT（信息技术）在未来必将得到广泛应用，IT更能体现个人价值，且学IT只需一台计算机。于是，我怀揣着对未来美好生活的期待，毅然决定改行，进军IT领域，开始学习IT。

从一名非计算机专业大学生到一位IT职业培训讲师，从IT菜鸟到出版了10多本计算机图书的作者，从化工技术员到微软最有价值专家，我历经20年，这期间有对学习IT持之以恒的坚持，也有对IT职业化培训的思考。面对互联网时代的到来，我敏锐地察觉到IT培训要和互联网结合，要通过互联网打破教学的时间和空间限制，尤其是2020年的新冠疫情，让互联网教育走向舞台。

由于自己是非计算机专业出身，从零基础开始学习计算机网络，后成为计算机网络相关课程的老师，因此非常了解零基础的学生学习计算机网络会遇到的困惑，所以我的授课内容易学易懂。我在微软高级培训中心经常给企业网管做培训，帮他们解决工作中的问题。我还录制了实战风格的网络课程，很多计算机专业的学生学习我的网络课程，也能感觉到我和学院派讲师的差别。

我听过很多老师的“计算机网络”课程，有些老师是参照书本制作PPT，上课照着PPT讲解，所讲内容仅限于书中的内容，对知识没有进一步扩展，和实际不进行关联，这其实和学生自己看书差不多。这

些老师尊重知识、尊重书本、尊重作者，但这种教学方式却没有尊重学生。作为老师，一定要了解学生，才能把课讲好。

我讲“计算机网络”课程20年，“计算机网络原理”课程12年，每一年都有新的提高，每一遍都有新的认识。如今我把对网络的认识写成书，用直白的语言、通俗的案例给大家阐述计算机网络技术，将实战融入理论。书中还讲解了如何使用华为路由器和交换机搭建计算机网络的学习环境。本书能够帮助读者掌握计算机网络通信理论，使用华为路由器和交换机组建企业局域网和广域网，熟练配置华为网络设备。

本书特色

相较于市面上已有的其他图书，本书具有如下特色。

- 理论与实践并重，用理论引导实践，用实践验证理论。
- 无须购买硬件设备，可使用eNSP软件来模拟网络设备，搭建学习环境。
- 一图胜千言。本书所讲的内容大多数配有形象的示意图，以降低读者的学习门槛。
- 每章配备课后习题，帮助读者夯实对内容的理解。
- 配有完备的PPT，进一步帮助读者理解、掌握本书内容。
- 配有QQ教学群（群号：301678170），解答学生问题，提供学习所需软件。

本书组织结构

本书共分为15章，主要内容如下所示。

- 第1章，认识计算机网络，讲解Internet的产生和发展、局域网组网设备的演进、企业局域网的规划和设计。
- 第2章，TCP/IP，介绍计算机通信使用的应用层协议、传输层协议、网络层协议和数据链路层协议。
- 第3章，IP地址和子网划分，介绍IP地址的组成和分类、子网划分和变长子网划分、使用超网合并网段。
- 第4章，管理华为设备，用eNSP搭建实验环境，通过Console口、telnet接口对路由器进行常规配置，创建登录账户和密码，管理路由器配置文件，使用抓包工具捕获链路中的数据包。
- 第5章，静态路由，讲解网络畅通的条件，在路由器上添加静态路由，通过路由汇总和默认路由简化路由表。
- 第6章，动态路由，介绍RIP的工作特点和OSPF协议的工作特点，配置路由器使用RIP和OSPF协议构造路由表。
- 第7章，交换机组网，讲解配置交换机的端口安全，使用生成树协议阻断交换机组网的环路，创建VLAN隔绝网络广播，使用三层交换和单臂路由器实现VLAN间路由。
- 第8章，网络安全，在路由器上创建基本访问控制列表和高级访问控制列表来实现数据包过滤，实现网络安全，使用ACL保护路由器telnet安全。
- 第9章，网络地址转换和端口映射，在路由器上配置NAPT，实现私网访问Internet，配置端口映射实现Internet访问内网服务器。

- 第10章，将路由器配置成DHCP服务器，配置路由器作为DHCP服务器为网络中的计算机分配IP地址，实现跨网段分配IP地址。
- 第11章，IPv6，讲解IPv6地址分类和地址格式，IPv6静态路由和动态路由，以及IPv6和IPv4共存技术。
- 第12章，广域网，介绍广域网链路使用的数据链路层协议，介绍HDLC、PPP、帧中继，将路由器配置为PPPoE客户端和PPPoE服务器。
- 第13章，VPN，介绍站点间VPN，配置GRE隧道VPN、IPSec VPN和基于tunnel接口的IPSec VPN，配置远程访问VPN。
- 第14章，WLAN技术，讲解什么是WLAN，WLAN业务分类、WLAN的标准，WLAN产品的演进，以及企业无线网络的配置。
- 第15章，园区网典型组网案例，本章是一个企业园区网典型组网案例，通过一个企业的具体场景，使用华为设备组建企业园区网，规划内网网段，部署有线和无线网络设备。

本书配套资源

除了纸质版图书，作者还为本书提供了完整的PPT以及配套的视频课程。PPT资源可通过本书在异步社区的相应页面进行下载，也可以向本书作者索要。与本书完全配套的视频课程，可到51CTO学院官方网站搜索“华为认证网络工程师（HCIA）”，找到韩立刚录制的课程然后进行访问（注意，视频课程为收费课程）。

由于作者水平有限，书中错漏之处在所难免，恳请广大读者批评指正。

致　　谢

首先感谢我们的祖国各行各业的快速发展，这为那些不甘于平凡的人提供了展现个人才能的平台。我很庆幸自己生活在这个时代。

互联网技术的发展为各行各业提供了广阔的舞台，感谢51CTO学院为全国的IT专家和IT教育工作者提供教学平台。

感谢我的学生们，正是他们的提问，才让我了解到学习者的困惑，也提升了我的授课水平。更感谢那些工作在一线的IT运维人员，帮他们解决工作中遇到的疑难杂症为我积累了许多专业的案例。

感谢那些深夜还在网上看视频学习我的课程的读者，虽然没有见过面，我却能够感受到你们怀揣梦想、想通过知识改变命运的决心和毅力，这也一直激励着我不断录制新课程、编著新书。

资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

配套资源

本书提供配套资源，请在异步社区本书页面中点击 

，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

如果您是教师，希望获得教学配套资源，请在社区本书页面中直接联系本书的责任编辑。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的100积分。积分可用于在异步社区兑换优惠券、样书或奖品。



与我们联系

我们的联系邮箱是contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问www.epubit.com/selfpublish/submission即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下IT专业图书社区，致力于出版精品IT技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于2015年8月，提供大量精品IT技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品IT专业图书的品牌，依托于人民邮电出版社近30年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。



异步社区



微信服务号

第1章　认识计算机网络

本章内容

- Internet的产生和中国的ISP
- 局域网的发展
- 企业局域网的规划和设计
- 通信领域常见的术语
- 传输媒体
- 网络分类

全球最大的互联网络就是Internet，本章讲解网络的产生以及Internet的发展，路由器在网络中的作用，以及中国的互联网和ISP。

企业网络管理员主要管理企业的局域网。本章开门见山地为你讲解局域网使用的协议、局域网组网设备的演进，还讲解了同轴电缆组建的局域网、集线器组建的局域网、网桥优化以太网、交换机组网。本章最后还讲解了典型的企业局域网的规划和设计，根据企业的计算机数量和物理位置，局域网可以设计成二层结构的局域网和三层结构的局域网。此外，本章还介绍了通信领域常见的术语，如带宽、延迟、吞吐量等；介绍了传输媒体，如导向传输媒体和引导性传输媒体；讲解了网络的分类（公网和私网或局域网和广域网）。

1.1　Internet的产生和中国的ISP

1.1.1　Internet的产生和发展

Internet是全球最大的互联网络，家庭通过电话线使用ADSL拨号上网接入的就是Internet，企业的网络通过光纤接入Internet，现在我们使用智能手机通过4G技术或5G技术也可以很容易接入Internet。Internet正在深刻地改变着我们的生活，网上购物、网上订票、预约挂号、QQ聊天、支付宝转账、共享单车等应用都离不开Internet。现在我们就讲解一下Internet的产生和发展过程。

最初计算机是独立的，没有相互连接，在计算机之间复制文件和程序很不方便，于是就用同轴电缆将一个办公室内（短距离、小范围）的计算机连接起来组成网络（局域网），计算机的网络接口卡（网卡）与同轴电缆连接，如图1-1所示。

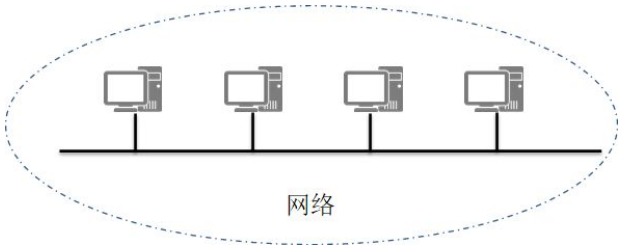


图1-1　网络

位于异地的多个办公室（如图1-2所示的Office1和Office2）的网络，如果需要通信，就要通过路由器连接，形成互联网。路由器有广

域网接口用于长距离数据传输，路由器负责在不同网络之间转发数据包。

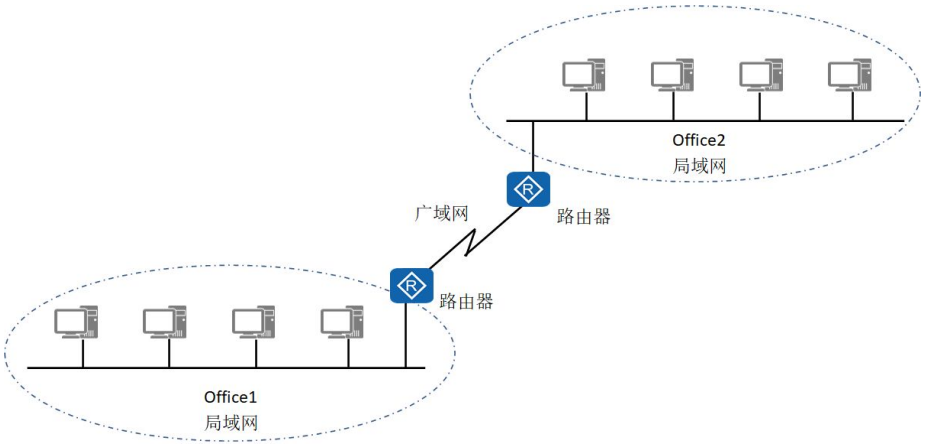


图1-2　路由器连接多个网络，形成互联网

最初只是美国各个大学和科研机构的网络进行互联，随后越来越多的公司、政府机构也接入网络。这个在美国产生的开放式的网络后来又不局限于美国，越来越多的国家网络通过海底光缆、卫星接入美国这个开放式的网络，如图1-3所示，就形成了现在的Internet，Internet是全球最大的互联网络。在这张图中你能体会到路由器的重要性，如何规划网络、配置路由器、为数据包选择最佳路径是网络工程师主要和重要的工作。当然，学完本书，你也能掌握对Internet的网络地址进行规划和简化路由器路由表的方法。

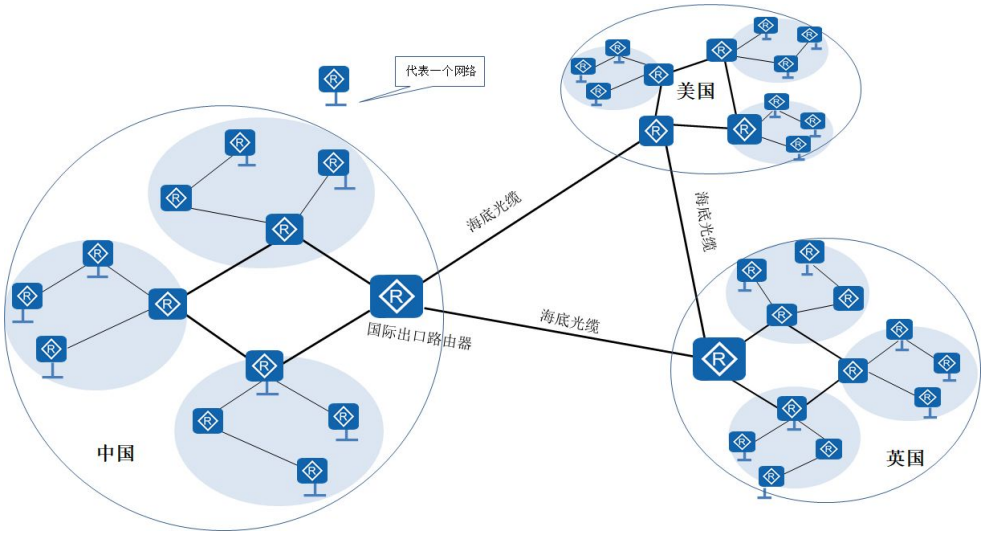


图1-3　Internet示意图

1.1.2　中国的ISP

Internet是全球网络，在中国主要有3家“互联网服务提供商”（Internet Service Provider，ISP），它们向广大用户和企业提供互联网接入业务、信息业务和增值业务。中国的三大互联网服务提供商分别是中国电信、中国移动、中国联通。

这些运营商在全国各大城市和地区铺设了通信光缆，用于计算机网络通信。运营商的作用就是为城镇居民、企业和机构提供Internet的接入服务，在大城市建立机房。小企业没有机房，可以购买服务器，将服务器托管到运营商的机房。用户和企业可以根据ISP所提供的网络带宽、入网方式、服务项目、收费标准以及管理措施等选择适合自己的ISP。

1.1.3　跨运营商访问网络带来的问题

Internet也就是因特网，是全球最大的互联网。我国主要有3家互联网服务提供商（ISP），他们向广大用户提供互联网接入业务、信息业务和增值业务。

中国三大基础运营商及其提供的服务如下所列。

- 中国电信：拨号上网、ADSL、1X、CDMA1X、EVDO rev.A、FTTx。
- 中国移动：GPRS及EDGE无线上网、TD-SCDMA无线上网，少部分FTTx。
- 中国联通：GPRS、W-CDMA无线上网、拨号上网、ADSL、FTTx。

下面以电信和联通两个ISP为例来展现Internet的局部组成，各个组织的网络和网民接入ISP的网络形成Internet。网站的连接示意如图1-4所示。

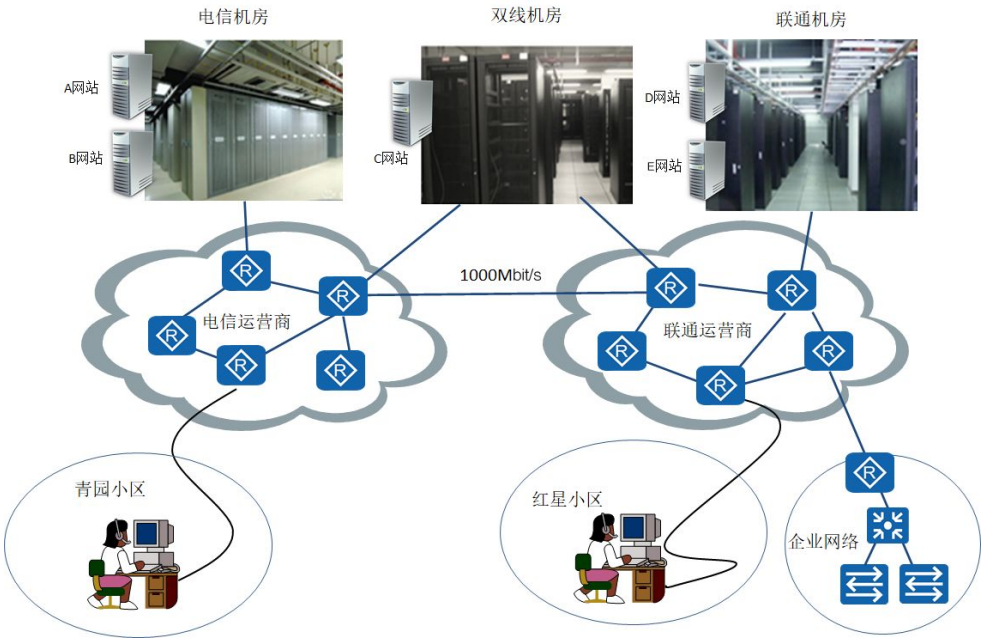


图1-4　各个组织的网络和网民接入ISP的网络形成Internet

ISP为家庭用户提供Internet接入服务，如图1-4所示，青园小区的用户光纤连接电信运营商，而红星小区使用光纤连接联通运营商。ISP也为企业网络提供Internet接入服务。

如果为企业服务器分配了公网地址，那么企业的网络就成为了Internet的一部分。

如果公司的网站需要为网民提供服务，自己又没有建设机房，就需要将服务器托管在联通和电信的机房，以提供7×24小时的高可用服务。机房不能轻易停电，需要保持无尘环境，并且温度、湿度、防火装置都有特殊要求，总之和家庭计算机的待遇不一样。

如图 1-4 所示，电信运营商和联通运营商之间使用 1000Mbit/s 的线路连接，虽然带宽很高，但其承载了所有联通访问电信的流量和电信访问联通的流量，因此还是拥堵。青园小区的用户访问A网站和B网站速度快，访问C网站和D网站的速度就会慢。

为了解决跨运营商访问网速慢的问题，可以把公司的服务器托管在双线机房，即同时连接联通和电信运营商网络的机房，如图1-4中的C网站部署在双线机房。这样用户通过联通或电信访问此类网站的速度没有差别。

有些Web站点会为用户提供软件下载功能，此时可以将软件部署到多个运营商的服务器中，让用户自己选择使用哪一个运营商下载。用户可以根据自家是联通上网还是电信上网来选择联通下载或电信下载，如图1-5所示。



图1-5　选择运营商

1.1.4　多层级的ISP结构

根据服务的覆盖面积大小以及所拥有的IP地址数目的不同，ISP也分为不同的层次。最高级别的第一层ISP为主干ISP，主干ISP的服务面积最大（一般都能覆盖国家范围），并且还拥有高速主干网。第二层ISP为地区ISP，一些大公司都属于第二层ISP的用户。第三层ISP又称为本地ISP，它们是第二层ISP的用户，且只拥有本地范围的网络。一般的校园网和企业网以及拨号上网的用户，都是第三层ISP的用户，如图1-6所示。

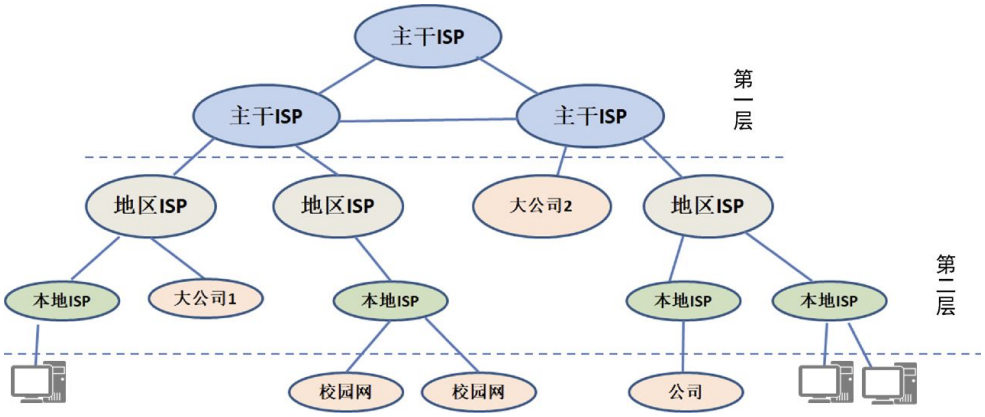


图1-6　多层级的ISP

比如中国联通是一级ISP，负责铺设全国范围内连接各地区的网络，中国联通有限公司石家庄分公司是地区ISP，负责石家庄地区的网络连接，石家庄联通藁城区分公司就属于三级ISP了，也就是本地ISP了。

如何理解ISP分级呢？比如你家通过联通的光纤接入Internet，带宽是100Mbit/s，上网费每年700元。你的3个邻居通过你家的路由器上网，每家每年给你300元上网费，你就相当于一个四级ISP了，你每年还能赢利200元。

有些公司的网站是为全国甚至全球提供服务的，比如淘宝网和12306网上订票网站，这样的网站最好接入主干ISP，全国网民访问主干网都比较快。有些公司的网站主要服务于本地区，比如58同城之类的网站，负责石家庄地区的网站就可以部署在石家庄地区的ISP机房。藁城区中学的网站主要是藁城区的学生和学生家长访问，藁城区中学的网站通过联通的本地ISP接入Internet。

网络规模大一点的公司接入Internet，ISP通常会部署光纤提供接入，家庭用户或企业小规模网络上网，ISP通常会通过电话线使用ADSL拨号提供Internet接入。随着光纤线路的普及，现在农村和城市的小区也可以使用光纤接入Internet了。

1.2　局域网的发展

本节讲解局域网的发展。先给大家介绍什么是局域网和广域网，再讲解局域网通信的特点以及使用的协议，最后介绍局域网组网设备，包括网卡、同轴电缆、集线器、网桥和交换机。

1.2.1　局域网和广域网

首先通过举例来简单了解一下局域网和广域网的概念。

中国电信运营商的网络覆盖全国，属于广域网。企业的网络通常覆盖一个厂区的几栋大楼，学校的网络覆盖整座学校。这种企业或学校自己组建的覆盖小范围的网络就是局域网。

除了最大的互联网——因特网，大多数企业也组建了自己的互联网。接下来介绍企业互联网拓扑，以加深读者对网络的认识。如图1-7所示，车辆厂在石家庄和唐山都有厂区。中车石家庄车辆厂和中车唐山机车车辆厂都组建了自己的网络，可以看到企业按部门规划网络，基本上是一个部门一个网段（网络），然后使用三层交换（相当于路由器）连接各个部门的网段，从而企业的服务器连接到了三层交换机，这就是企业的局域网。

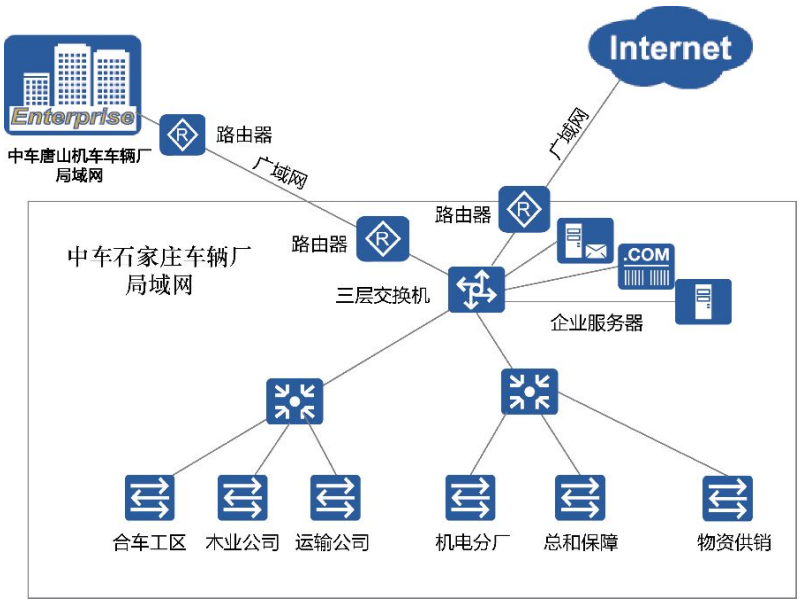


图1-7　企业互联网

一个车辆厂需要访问另一个车辆厂的服务器，这就需要将这两个厂区的网络连接起来。车辆厂不可能自己架设网线或光纤来将这两个厂区的局域网连接起来，架设和维护的成本太高了。车辆厂租用了联通的线路来将两个局域网连接起来，只需每年缴费即可，连接后的局域网就是广域网。中车石家庄车辆厂使用网通的光纤来连接Internet，这也是广域网。

现在总结一下，局域网通常是公司或单位自己花钱购买网络设备组建，带宽通常为10Mbit/s、100Mbit/s或1000Mbit/s，自己维护，覆盖范围小。广域网通常要花钱租用联通、电信等运营商的线路，花钱买带宽，用于长距离通信。

1.2.2　同轴电缆组建的局域网

早期的计算机网络就是使用一根同轴电缆连接网络中的计算机，计算机之间的通信信号会被同轴电缆传送到所有计算机，所以说同轴电缆是广播信道，如图1-8所示。

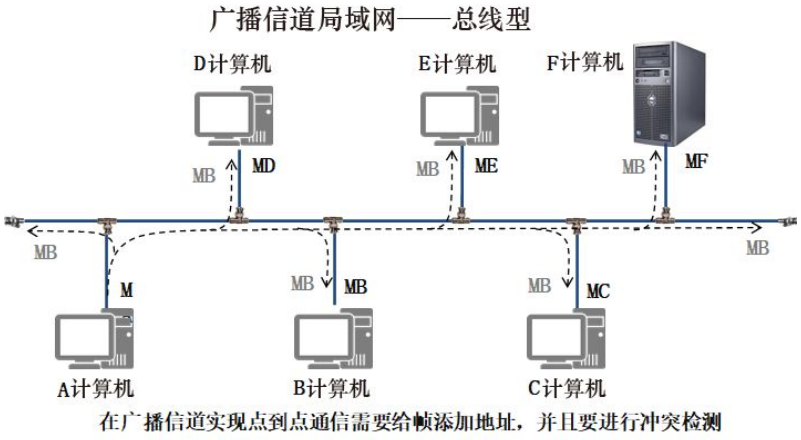


图1-8　广播信道局域网——总线型

在这样的广播信道里，如何实现点到点通信呢？那就需要通信的计算机都有一个地址，这个地址就是网卡的MAC地址。如果这些计算机发现收到的数据帧的目标MAC地址和自己网卡的MAC地址不一样，就丢弃这个数据帧。

MAC（Media Access Control或者Medium Access Control）地址可意译为媒体访问控制，或称为物理地址、硬件地址，用来定义网络设备的位置。

同轴电缆上连接的这些计算机不允许多台计算机同时发送数据，如果多台计算机同时发送数据，发送的信号就会叠加造成信号不能正

确识别。所以计算机在发送数据之前先侦听网络中有没有数据在传输，发现没有信号传输才发送数据，这就是载波侦听。

即便在开始发送的时候没有检测出有信号在传输，在开始发送后，也有可能在同轴电缆的某处和其他计算机发送的信号迎面相撞，发送端收到相撞后的信号会认为发送失败。发送端必须能够检测出这种发生在链路上的冲突，然后通过退避算法来计算退避时间并尝试再次发送，这就是冲突检测。

这种使用共享介质进行通信的网络，网络中的设备接口必须有MAC地址，每台计算机发送数据的机会均等（多路访问，Multiple Access），发送之前检测链路是否有信号在传输（载波侦听，Carrier Sense）。即便开始发送了，也要检测链路上是否产生冲突（冲突检测，Collision Detection），这种带冲突检测的载波侦听多路访问机制就是CSMA/CD协议，使用CSMA/CD协议的网络就是以太网。局域网通常使用共享介质线路组建，使用CSMA/CD协议通信，所以有人不严谨地说局域网就是以太网，但你应该知道以太网的实质和局域网的实质，使用CSMA/CD协议的是以太网，覆盖小范围的网络是局域网。

1.2.3 集线器组建的局域网

同轴电缆随后被集线器（HUB）这种设备替代，使用双绞线可以很方便地将计算机接入到网络中。其功能和同轴电缆一样，只是负责将一个接口收到的信号扩散到全部接口，计算机通信依然共享介质，使

用的依然是CSMA/CD协议，因此使用集线器组建的网络也被称为以太网，如图1-9所示，图中的MA、MB、MC和MD代表计算机的MAC地址。

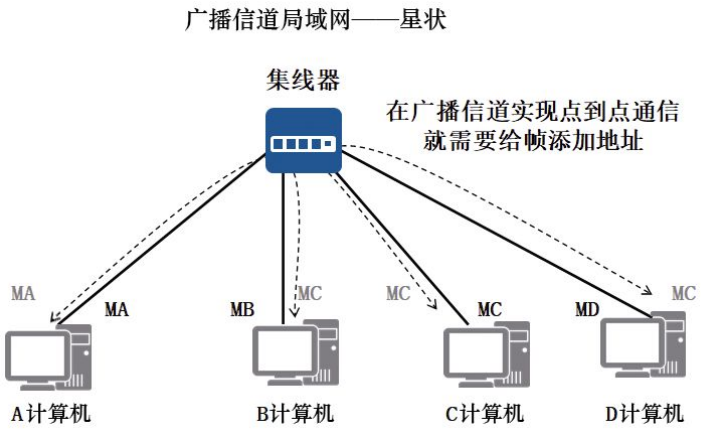


图1-9　集线器组建的以太网

使用集线器和同轴电缆组网具有如下特点。

- 网络中的计算机共享带宽，如果集线器带宽是10Mbit/s，网络中有4台计算机，理想状态下平均每台计算机的通信带宽是2.5Mbit/s。可见以太网中计算机数量越多，平均到每台计算机的带宽越少，理想状态是不考虑产生冲突后重传浪费的时间。
- 不安全，由于集线器会把一个接口收到的信号传播到全部接口，在一台计算机上安装抓包软件就能够捕获以太网中全部的计算机通信流量。安装抓包软件之后，只要网卡收到的数据帧就接收，而不看目标MAC地址是否是自己。
- 使用集线器联网的计算机就在冲突域中，通信要避免冲突。
- 接入集线器的设备需要有MAC地址。
- 使用CSMA/CD协议进行通信。
- 每个接口的带宽相同。

1.2.4　网桥优化以太网

如果网络中的计算机数量太多，就将计算机接入多个集线器，再将集线器连接起来。集线器相连可以扩大以太网的规模，但随之而来的一个问题就是冲突的增加。如图1-10所示，集线器1和集线器2相连，形成了一个大的以太网，这两个集线器就形成了一个大的冲突域。A计算机和B计算机通信的数据也被传输到集线器2的全部接口，D计算机和E计算机就不能通信了，冲突域变大，冲突增加。

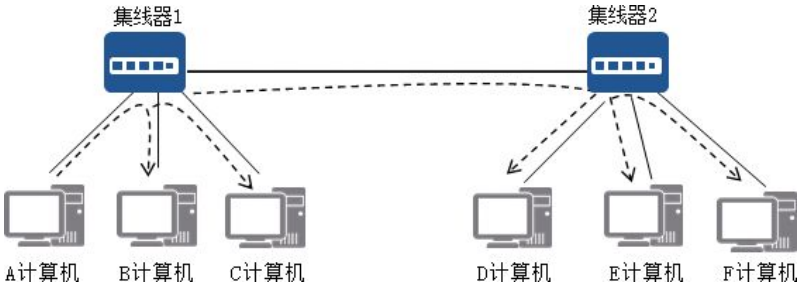


图1-10　扩展的以太网

为了解决集线器级联冲突域增大的问题，研究人员研发了网桥这种设备，用网桥的每个接口连接一个集线器。网桥能够构造MAC地址表，记录每个接口对应的MAC地址，如图1-11所示。网桥的E0接口连接集线器1，集线器1上连接3台计算机，这3台计算机的MAC地址分别为MA、MB和MC，于是网桥就在MAC地址表中记录E0接口对应MA、MB和MC 3个MAC地址。E1接口连接集线器2，集线器2连接的3台计算机的MAC地址分别是MD、ME和MF，于是在MAC地址表中E1接口对应MD、ME和MF 3个MAC地址。

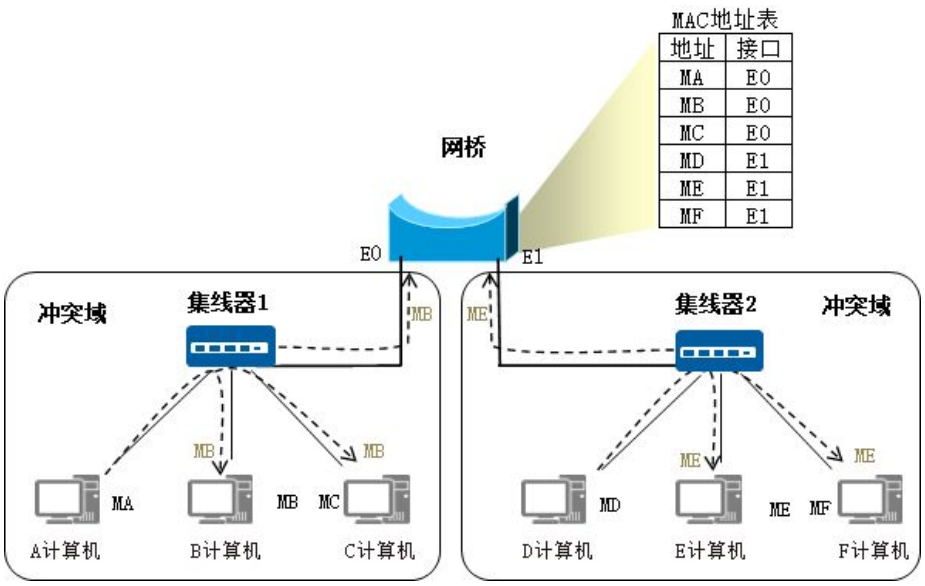


图1-11　网桥优化以太网

有了MAC地址表，A计算机发送给B计算机的帧被传输到网桥的E0接口，网桥查MAC地址表后发现目标MAC对应的接口就是E0，该帧就不会转发到E1接口。这时D计算机也可以向E计算机发送数据了。这样网桥就把一个大的冲突域划分成了两个小的冲突域，从而优化了集线器组建的以太网。

如果A计算机向D计算机发送帧，网桥会根据帧的目标MAC地址来对照MAC地址表以确定转发端口，从E1接口发送出去。当然，从E1接口发送出去时，计算机也要冲突检测载波侦听，寻找机会发送出去。

网桥组网有以下特点。

- 网桥基于帧的目标MAC地址选择转发端口。
- 一个接口一个冲突域，冲突域数量增加，冲突减少。
- 网桥接口收到一个帧后，先接收存储，再查MAC地址表选择转发端口，增加了时延。

- 网桥接口E1和E2的带宽可以不同，集线器所有接口的带宽一样。

1.2.5　网桥MAC地址表构建过程

若使用网桥优化以太网，那么网络中的计算机是无法识别该操作的，也就是说以太网中的计算机并不知道网络中有网桥存在，因此也不需要网络管理员配置网桥的MAC地址表。这时，我们称网桥是透明桥接。

网桥接入以太网时，MAC地址表是空的，网桥会在计算机通信过程中自动构建MAC地址表。这叫作“自学习”。网桥通过自学习构建MAC地址表，再根据MAC地址表转发帧。

（1）自学习。

网桥的接口收到一个帧后，就要检查MAC地址表中有无与收到的帧源MAC地址匹配的项。如果没有，就在MAC地址表中添加该接口与该帧的源MAC地址之间的对应关系以及进入接口的时间；如果有，则对原有的项目进行更新。

（2）转发帧。

网桥接口收到一个帧后，就要检查MAC地址表中有没有该帧目标MAC地址的对应端口。如果有，就将该帧转发到对应的端口；如果没有，则将该帧转发到全部端口（接收端口除外）。如果转发表中给出

的接口就是该帧进入网桥的接口，则应该丢弃这个帧（因为这个帧不需要经过网桥进行转发）。

下面举例说明MAC地址表的构建过程，如图1-12所示。网桥1和网桥2刚刚接入以太网，此时MAC地址表是空的。

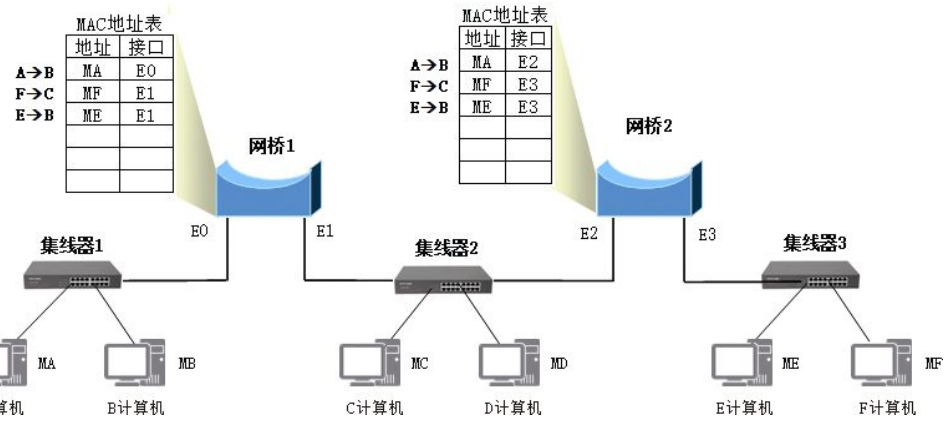


图1-12　构建MAC地址表的过程

（1）计算机A给计算机B发送一个帧，源MAC地址为MA，目标MAC地址为MB。网桥1的E0接口收到该帧，查看该帧的源MAC地址是MA，就可以断定E0接口连接MA，于是在MAC地址表中记录一条对应关系——MA和E0。这就意味着以后要有到达MA的帧，就需要转发给E0。

（2）网桥1在MAC地址表中没有找到MB和接口的对应关系，就会将该帧转发到E1。

（3）网桥2的E2接口收到该帧，查看该帧的源MAC地址，然后在MAC地址表中记录一条MA和E2的对应关系。

（4）这时，计算机F给计算机C发送一个帧，这会在网桥2的MAC地址表添加一条MF和E3的对应关系。由于网桥2的MAC地址表中没有MC和接口的对应关系，所以该帧会被发送到E2接口。

（5）网桥1的E1接口收到该帧，这会在MAC地址表中添加一条MF和E1的对应关系，同时将该帧发送到E0接口。

（6）同样，计算机E给计算机B发送一个帧，会在网桥1的MAC地址表中添加ME和E1的对应关系，在网桥2的MAC地址表中添加ME和E3的对应关系。

只要网桥收到的帧的目标MAC地址能够在MAC地址表找到和接口的对应关系，该帧就会被转发到指定接口。

网桥MAC地址表中的MAC地址和接口的对应关系只是临时的，这是为了适应网络中的计算机出现的调整，比如连接在集线器1上的计算机A连接到了集线器2，或者计算机F从网络中移除了，网桥中的MAC地址表中的条目就不能一成不变。大家需要知道，接口和MAC地址的对应关系有时间限制，如果过了几分钟没有使用该对应关系转发帧，该条目将会从MAC地址表中删除。

1.2.6　交换机组网

随着技术的发展，网桥接口越来越多，数据的交换能力也越来越强。这种高性能网桥我们称为交换机（Switch），交换机是现在企业组网的主流设备。

交换机和网桥一样，可以构造MAC地址表，并基于MAC地址转发帧。如图1-13所示，由于交换机直接连接计算机，因此A计算机给B计算机发送数据不影响D计算机给C计算机发送数据。如果两台计算机同时向B计算机发送数据，会不会产生冲突呢？答案是，不会。

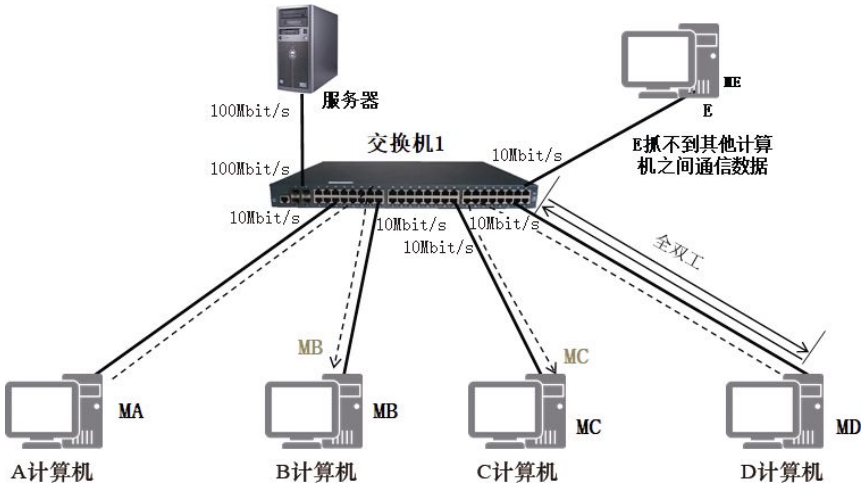


图1-13　交换机组网

交换机的每个接口都可以接收缓存和发送缓存，帧可以在缓存中排队。接收到的帧先进入接收缓存，再查找MAC地址表以确定转发端口，然后进入转发端口的发送缓存，排队等待发送。因此，多台计算机同时给一台计算机发送数据，数据会进入缓存排队等待发送，而不会产生冲突。正因为交换机使用的是存储转发，所以交换机的接口可以工作在不同的速率下。

使用交换机组网比集线器和同轴电缆更安全，如图1-13所示，E计算机即便安装了抓包软件，也不能捕获A计算机给B计算机发送的帧，因为交换机根本不会将帧转发给E计算机。

计算机的网卡直接连接交换机的接口，它可以工作在全双工模式下，即可以同时发送和接收帧而不用冲突检测。集线器和同轴电缆组建的以太网只能工作在半双工模式下，即不能同时收发。

如果交换机收到一个广播帧，即目标MAC地址是FF-FF-FF-FF-FF-FF的数据帧，交换机将该帧发送到所有交换机端口（除发送端口），因此交换机组建的网络就是一个广播域。

MAC地址由48位二进制数组成，F是十六进制数，F代表4位二进制数1111。

与集线器组网相比，交换机组网有以下特点。

- 端口独享带宽。

交换机的每个端口独享带宽，10Mbit/s交换机每个端口的带宽是10Mbit/s，24个10Mbit/s交换机的总体交换能力是240Mbit/s，这和集线器不同。

- 安全。

使用交换机组建的网络比使用集线器组建的安全，比如计算机A发送给计算机B的帧，以及计算机D发送给计算机C的帧，交换机根据MAC地址表只转发到目标端口，E计算机根本收不到其他计算机通信的数字信号，即便安装了抓包工具也没用。

- 全双工通信。

交换机接口和计算机直接相连，计算机和交换机之间的链路可以使用全双工通信。

- 全双工不再使用CSMA/CD协议。

交换机接口和计算机直接相连，使用全双工通信的数据链路层就不再需要使用CSMA/CD协议，但我们还是称交换机组建的网络是以太网，是因为帧格式和以太网的一样。

- 接口可以以不同的速率工作。

交换机使用的是存储转发，这意味着交换机的每一个接口都可以存储帧，从其他端口转发出去时，可以使用不同的速率。通常连接服务器的接口要比连接普通计算机的接口带宽高，交换机连接交换机的接口也比连接普通计算机的接口带宽高。

- 转发广播帧。

广播帧会转发到除了发送端口以外的全部端口。广播帧就是指的目标MAC地址的48位二进制全是1。

使用交换机组网，计算机通信可以设置成全双工模式，可以同时收发，不需要冲突检测，因此也不需要使用CSMA/CD协议。因为交换机转发的帧和以太网的帧格式相同，所以我们依然习惯说交换机组建的网络是以太网。

如图1-14所示，路由器连接两个交换机，交换机连接计算机和集线器，路由器隔绝广播，图中标出了广播域和冲突域。

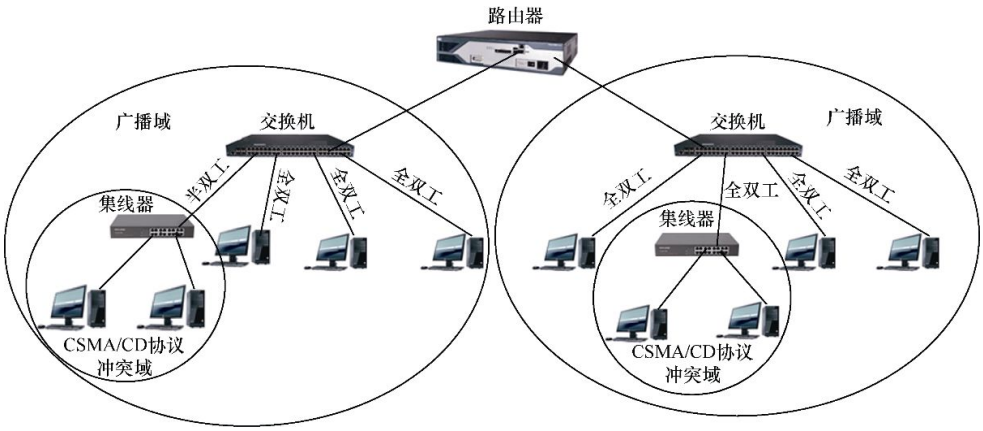


图1-14　广播域和冲突域

1.2.7　以太网网卡

为了在广播信道中实现点到点通信，需要网络中的每个网卡有一个地址。这个地址称为物理地址或MAC地址（因为这种地址用在MAC帧中）。IEEE 802标准为局域网规定了一种48位二进制的全球地址。

在生产网卡时，这种48位二进制（占6字节）的MAC地址已被固化在网卡的ROM中。因此，MAC地址也称为硬件地址或物理地址。当把这块网卡插入（或嵌入）某台计算机后，网卡上的MAC地址就成为这台计算机的MAC地址了。

如何确保各网卡生产厂家生产的网卡的MAC地址全球唯一呢？这就要有一个组织为这些网卡生产厂家分配地址块。现在IEEE的注册管理机构RA是局域网全球地址的法定管理机构，它负责分配地址字段的6字

节中的前3字节（高位24位）。世界上凡要生产局域网网卡的厂家都必须向IEEE购买由这3字节构成的号（即地址块），这个号的正式名称是组织唯一标识符，通常也叫作公司标识符。例如，如图1-15所示，3Com公司生产的网卡的MAC地址的前3字节是02-60-8C（在计算机中是以十六进制显示的）。地址字段中的后3字节（低位24位）则由厂家自行指派，它称为扩展标识符，只要保证生产出的网卡没有重复地址即可。由此可见，用一个地址块可以生成2^{24}个不同的地址。

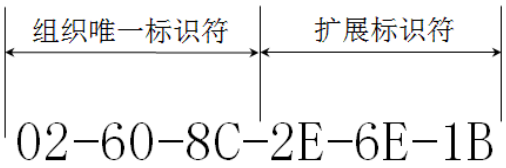


图1-15　3Com公司生产的网卡的MAC地址

连接在以太网上的路由器接口和计算机网卡的一样，也有MAC地址。

网卡有帧过滤功能，网卡从网络上每收到一个MAC帧，就先用硬件检查MAC帧中的目的地址。如果是发往本站的帧，则收下，然后进行其他的处理；否则就将此帧丢弃，不再进行其他的处理。这样做不浪费主机的CPU和内存资源。这里“发往本站的帧”包括以下3种帧。

- 单播（unicast）帧（一对一），即收到的帧的MAC地址与本站的硬件地址相同。
- 广播（broadcast）帧（一对全体），即发送给本局域网上所有计算机的帧（目标MAC地址全1）。

- 多播（multicast）帧（一对多），即发送给本局域网上一部分计算机的帧。

所有的网卡都至少应当能够识别前两种帧，即能够识别单播地址和广播地址。有的网卡可用编程方法识别多播地址。当操作系统启动时，它就把网卡初始化，使网卡能够识别某些多播地址。显然，只有目的地址才能使用广播地址和多播地址。

在Windows中查看网卡MAC地址的命令如下：

C:\Users\hanlg>ipconfig /all

以太网适配器 以太网:

媒体状态 . . . . . : 媒体已断开连接

连接特定的DNS后缀 . . . . . :

描述. . . . . : Realtek PCIe GBE Family Controller

物理地址. . . . . : F4-8E-38-E7-37-8B --MAC地址

……

1.3　企业局域网的规划和设计

根据网络规模和物理位置，企业的网络可以设计成二层结构或三层结构。通过本节的学习，你能掌握企业内网的交换机如何部署和连接，以及服务器部署的位置。

1.3.1　二层结构的局域网

现在以某高校网络为例介绍校园网的网络拓扑。如图1-16所示，在教室1、教室2和教室3分别部署一台交换机，对教室内的计算机进行连接。教室中的交换机要求端口多，这样能够将更多的计算机接入网络，这一级别的交换机称为接入层交换机，接计算机的端口带宽为100Mbit/s。

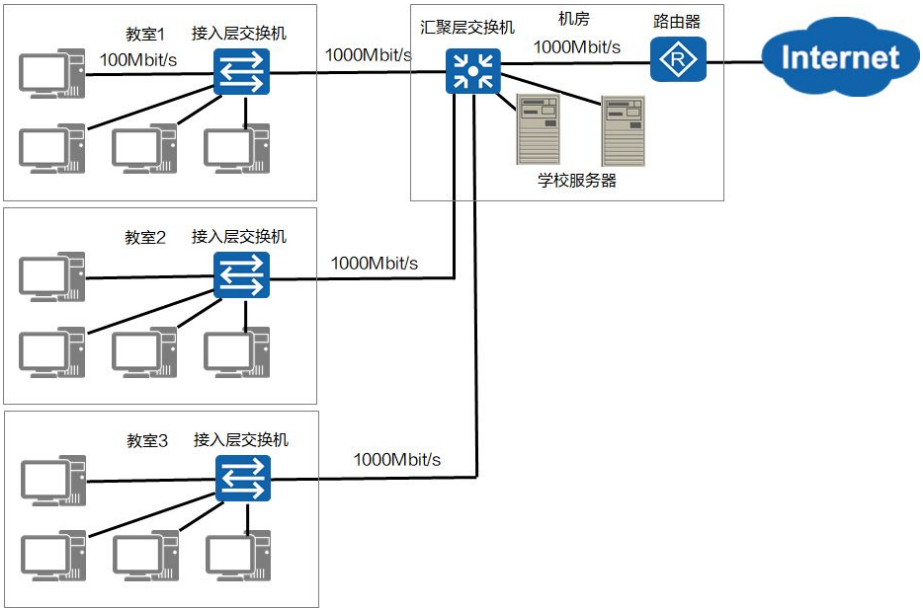


图1-16　二层结构的局域网

学校机房部署一台交换机，该交换机连接学校的服务器和教室中的交换机，并通过路由器连接Internet。该交换机汇聚教室中交换机的上网流量，该级别的交换机称为汇聚层交换机。可以看到这一级别的交换机端口不一定太多，但端口带宽要比接入层交换机的带宽高，否则就会成为制约网速的瓶颈。

1.3.2 三层结构的局域网

在网络规模比较大的学校中，局域网可能采用三层结构。如图1-17所示，某高校有3个学院，每个学院有自己的机房和网络，学校网络中心为3个学院提供Internet接入，各学院的汇聚层交换机连接到网络中心的交换机，网络中心的交换机称为核心层交换机，学校的服务器接入核心层交换机，为整个学校提供服务。

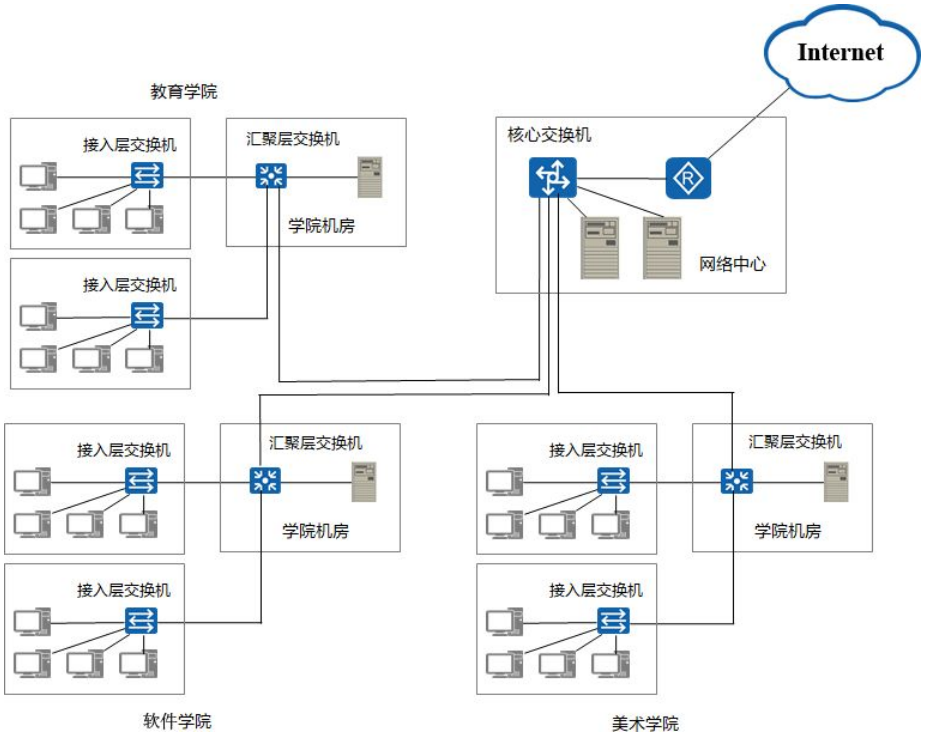


图1-17　三层结构的局域网

三层结构的局域网中的交换机有3个级别：接入层交换机、汇聚层交换机和核心层交换机。层次模型可以用来帮助设计，实现和维护可扩展、可靠、性价比高的层次化互联网络。

1.4　通信领域常见的术语

1.4.1　速率

计算机通信需要将发送的信息转换成二进制数字来传输，一位二进制数称为一个比特（bit）。二进制数字要转换成数字信号在线路上传输，如图1-18所示。

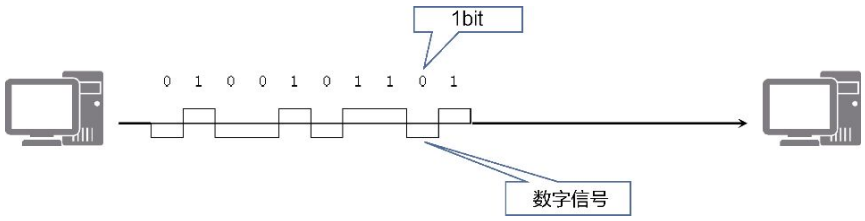


图1-18　二进制数与数字信号

网络技术中的速率指的是每秒传输的比特数量，也叫作数据率（data rate）或比特率（bit rate），速率的单位为b/s（比特每秒）或bit/s。当速率较高时，可以用kb/s（k=10^3，千）、Mbit/s（M=10^6，兆）、Gbit/s（G=10^9，吉）或Tbit/s（T=10^{12}，太）来表示。现在人们习惯用更简洁但不严格的说法来描述速率，比如10M网速，而省略了单位中的bit/s。

在Windows操作系统中，速率以字节为单位。如果安装了测速软件，比如360安全卫士，就有带宽测速器，可以用来检测你的计算机访问Internet时的下载网速。不过这里的单位是B/秒，大写的B代表字

节，是byte的缩写，8比特=1字节。如果测速为3.82MB/s，则下载速率为3.82 MB/s×8，即30.56Mbit/s。

如图1-19所示，我们在Windows 7中复制文件时，可以看到以字节为单位的速率。它转换成以比特为单位的速率时要乘8，因此一定要注意速率是大写的B还是小写的b。

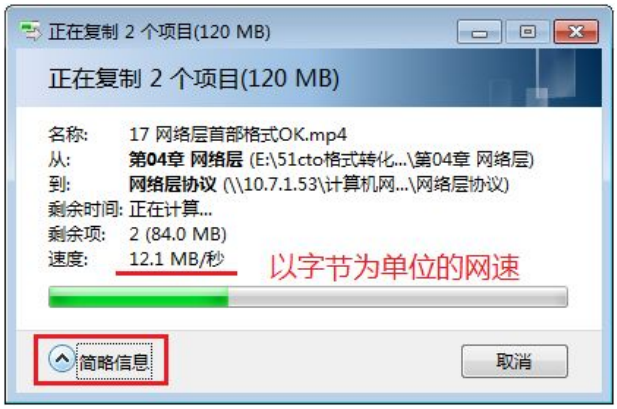


图1-19　操作系统的网速以字节为单位

1.4.2　带宽

在通信领域，带宽用来表示接口或通信线路传输数据的能力，即最高速率。图1-20所示的是便携式笔记本网卡的本地连接，可以看到速率为100.0Mbps（100.0Mbit/s），说明网卡最快每秒传输100Mbit。再比如家庭上网使用ADSL拨号，有4Mbit/s带宽、8Mbit/s带宽，这里说的带宽是访问Internet的最高带宽，上网带宽要由电信运营商来控制。



图1-20　本地连接带宽

1.4.3　吞吐量

吞吐量表示在单位时间内通过某个网络或接口的数据量，包括上传和下载的全部流量。如图1-21所示，计算机A同时进行3个操作：浏览网页，在线看电影，向FTP服务器上传文件。访问网页的下载速率为30Kb/s，播放视频的下载速率为40Kb/s，向FTP上传文件速率为20Kb/s，A计算机的吞吐量就是全部上传下载速率总和，即30+40+20=90（kbit/s）。

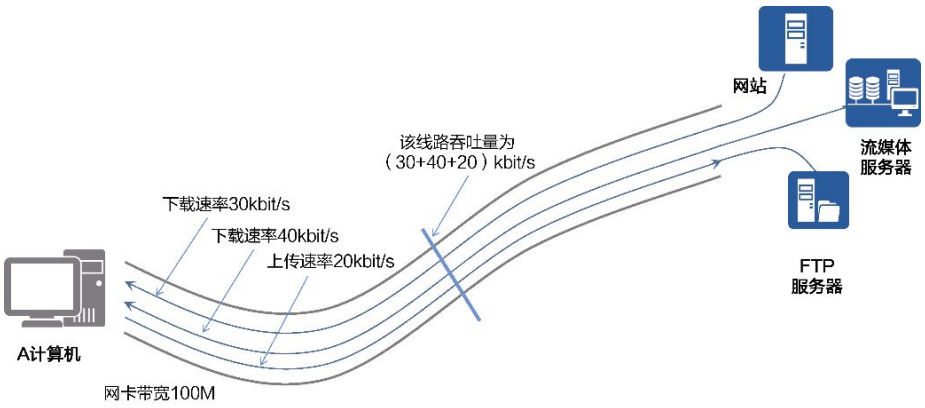


图1-21　吞吐量

吞吐量受网络带宽或网络额定速率的限制。计算机的网卡如果连接交换机，那么网卡就可以在全双工模式下工作，即能够同时接收和发送数据。如图1-22所示，如果网卡在100Mbit/s的全双工模式下工作，就意味着网卡的最大吞吐量为200Mbit/s。

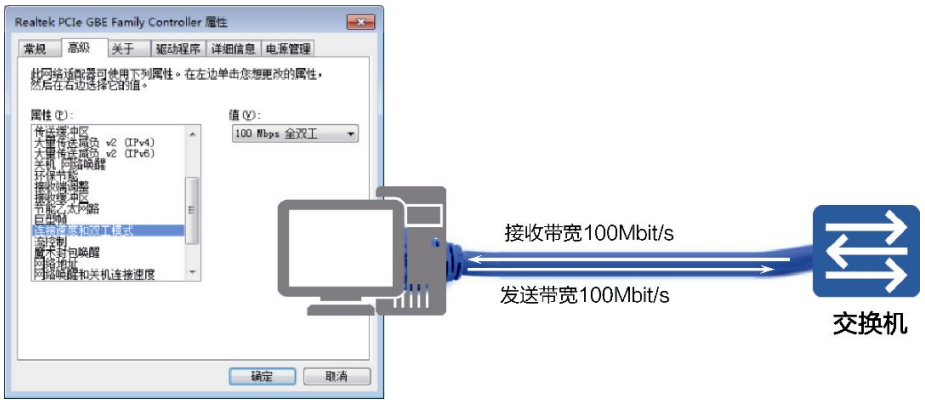


图1-22　全双工吞吐量

如果计算机的网卡工作在半双工模式下，那么就不能同时发送和接收数据。网卡工作在100M半双工模式，则网卡的最大吞吐量为100Mbit/s。

1.4.4 时延

时延（delay或latency）是指数据（一个数据包或bit）从网络的一端传送到另一端所需要的时间。时延是一个很重要的性能指标，有时也称为延迟或迟延。

接下来就以计算机A给计算机B发送数据为例，来说明网络中的时延包括哪几部分，如图1-23所示。

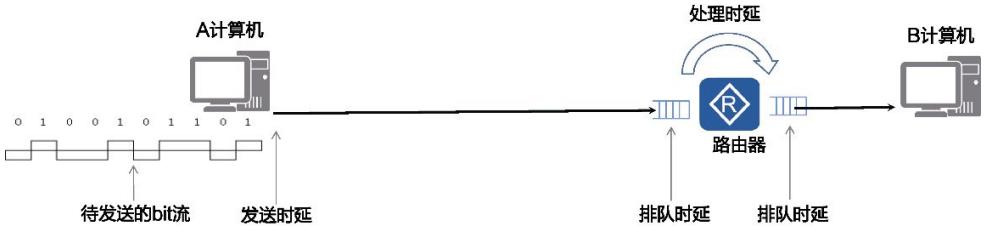


图1-23　各种时延

（1）发送时延。

发送时延（transmission delay）是主机或路由器发送数据帧所需的时间，也就是从发送数据帧的第一个比特开始，到该帧最后一个比特发送完毕所需要的时间。图1-24表示数据流发送完毕。

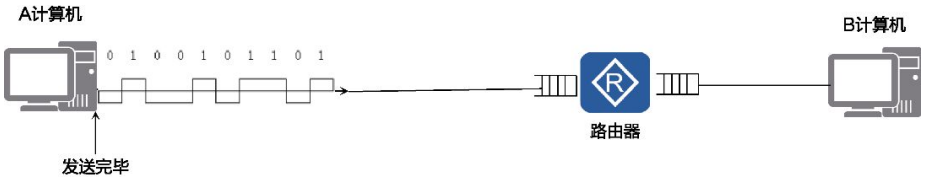


图1-24　发送时延

$$\text{发送时延} = \frac{\text{数据帧长度 (bit)}}{\text{发送速率 (bit/s)}}$$

可以看到发送时延和数据帧的长度以及发送速率有关，发送速率就是网卡的带宽，100Mbit/s的网卡就意味着1秒能够发送100×10^6比特。

以太网最大的数据帧为1518字节，再加上8字节前导字符，共计1526字节，即1526×8=12208比特。网卡带宽如果是10Mbit/s，发送一个最大以太网数据帧的$\text{发送延迟} = \frac{12208}{10000000} = 1.2\ \text{ms}$。

（2）传播时延。

传播时延（propagation delay）是指电磁波在信道中传播一定的距离需要花费的时间。如图1-25所示，$t1$时刻最后一比特发送完毕，$t2$时刻路由器收到最后一比特，$t2-t1$就是传播时延。

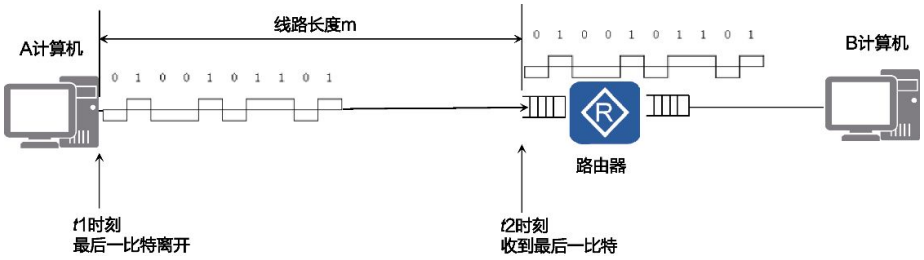


图1-25　传播时延

$$\text{传播时延} = \frac{\text{信道长度 (m)}}{\text{电磁波在信道上的传播速率 (m/s)}}$$

电磁波在自由空间中的传播速度是光速，即3.0×10^5km/s。电磁波在网络中的传播速度要比在自由空间中略低一些：在铜线电缆中的传播速率约为2.3×10^5km/s，在光纤中的传播速率约为2.0×10^5km/s。例如在1000km长的光纤线路产生的传播时延大约为5ms。

电磁波在指定介质中的传播速率是固定的，从公式可以看出，信道长度固定了，传播时延也就固定了，我们没有办法改变。

网卡的不同带宽改变的只是发送时延，而不是传播时延。如图1-26所示，4Mbit/s带宽网卡发送10比特需要2.5μs，2Mbit/s带宽网卡发送10比特需要5μs。1s（秒）=1000ms（毫秒）= 1000000μs（微秒）。如果同时从A端向B端发送，4Mbit/s网卡发送完10比特，而2Mbit/s网卡刚刚发送完5比特。

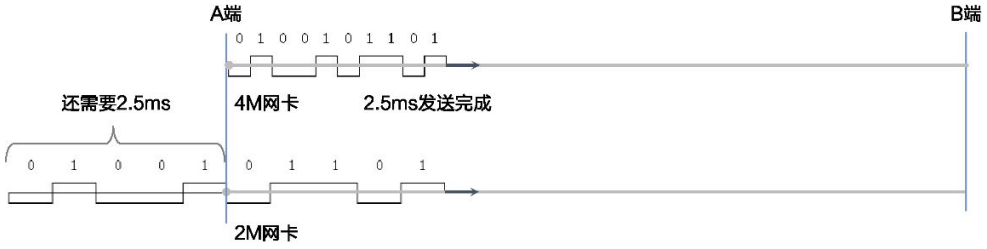


图1-26　带宽和发送时延的关系

（3）排队时延。

数据分组在经过网络传输时要经过许多的路由器。但数据分组在进入路由器后要先在输入队列中排队等待处理。在路由器确定了转发接口后，还要在输出队列中排队等待转发，这就产生了排队时延。排

队时延的长短往往取决于网络当时的通信量。当网络的通信量很大时会发生队列溢出，使分组丢失，这相当于排队时延为无穷大。

（4）处理时延。

路由器或主机在收到数据包时，要花费一定的时间对其进行处理，例如分析数据包的首部、进行首部差错检验、查找路由表为数据包选定的转发出口，这就产生了处理时延。

数据在网络中经历的总时延就是以上4种时延的总和：

总时延=发送时延+传播时延+处理时延+排队时延

1.4.5 时延带宽积

把链路上的传播时延和带宽相乘，就会得到时延带宽积。

时延带宽积=传播时延×带宽

这个指标用来计算通信线路上有多少比特。下面我们通过案例来看看时延带宽积的意义。

如图1-27所示，A端到B端是1km的铜线路，电磁波在铜线中的传播速率为2.3×10^5km/s，在1km长的铜线传播时延大约为4.3×10^{-6}s。A端网卡带宽为10Mbit/s，A端向B端发送数据时，问链路上有多少比特？我们只需要计算4.3×10^{-6}s的时间内A端网卡发送多少比特即可得出链路上有多少比特，这就是时延带宽积。

时延带宽积=4.3×10^6s×10×10^6bit/s=43bit，进一步计算得出每比特在铜线中的长度是23m。

如果发送端的带宽为100Mbit/s，则时延带宽积=4.3×10^6s×100×10^6bit/s=430bit。这意味着1km铜线中可以容纳430bit，每比特2.3m。

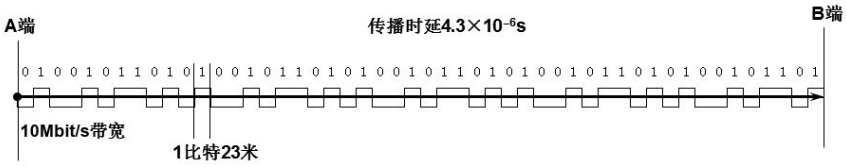


图1-27　时延带宽积

1.4.6　往返时间

在计算机网络中，往返时间（Round-Trip Time，RTT）也是一个重要的性能指标，它表示从发送端发送数据开始，到发送端接收到来自接收端的确认（接收端收到数据后立即发送确认）为止，总共经历的时间。

往返时间带宽积，可以用来计算当发送端连续发送数据时，接收端如果发现有错误立即向发送端发送通知使发送端停止发送数据，发送端在这段时间所发送的比特量。

在Windows操作系统中使用ping命令也可以显示往返时间。如图1-28所示，我们分别ping 网关、国内的网站和美国的网站，可以看到每

一个数据包的往返时间和系统统计的平均往返时间，可以看到途经的路由器越多、距离越远，往返时间也会越长。

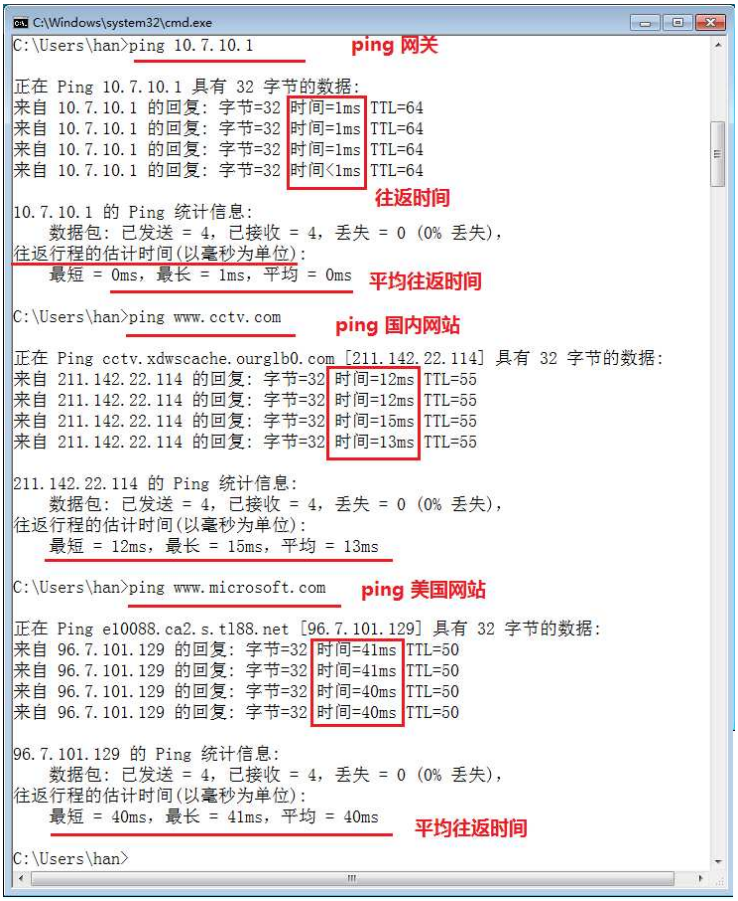


图1-28　往返时间

经验分享：通常情况下，企业内网之间计算机ping的往返时间小于10ms。如果大于10ms，就要安装抓包工具来分析网络中的数据包是否有恶意的广播包，以找到发广播包的计算机。

1.4.7　利用率

利用率是指网络有百分之几的时间是被利用的（有数据通过），没有数据通过的网络的利用率为零。网络利用率越高，数据分组在路由器和交换机处理时就需要排队等待，因此时延也就越大。下面的公式可以表示网络利用率和延迟之间的关系。

$$D = \frac{D_0}{1 - U}$$

U是网络利用率，D表示网络当前时延，D_0表示网络空闲时的时延。图 1-29 所示为网络利用率和时延之间的关系，当网络的利用率接近最大值1时，网络的时延就趋于无穷大。因此，一些拥有较大主干网的ISP通常要控制它们的信道利用率不超过50%。如果超过了就要准备扩容，以增大线路的带宽。

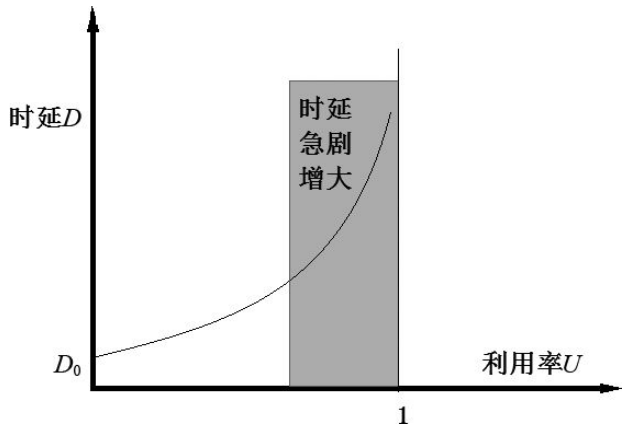


图1-29　时延和网络利用率

1.5　传输媒体

传输媒体也称为传输介质或传输媒介，它就是数据传输系统中发送器和接收器之间的物理通路。传输媒体可分为两大类，导向传输媒体（也称为导引型传输媒体）和非导向传输媒体（非导引型传输媒体）。在导向传输媒体中，电磁波被导向沿着固体媒体（铜线或光纤）传播，而非导向传输媒体就是指自由空间，在非导向传输媒体中电磁波的传输常称为无线传输。

1.5.1　导向传输媒体

1. 双绞线

双绞线也称为双扭线，它是最古老但又是最常用的传输媒体。把两根互相绝缘的铜导线并排放在一起，然后用规则的方法绞合（twist）起来就构成了双绞线。这种方式不仅可以抵御一部分来自外界的电磁波干扰，也可以降低多对绞线之间的相互干扰。使用双绞线最多的地方就是到处都有的电话系统。几乎所有的电话都用双绞线连接到电话交换机。这段从用户电话机到交换机的双绞线称为用户线或用户环路。通常将一定数量的双绞线捆成电缆，然后在其外面包上护套。

模拟传输和数字传输都可以使用双绞线，其通信距离一般为几千米到十几千米。距离太长时就要加放大器以便将衰减的信号放大到合

适的数值（对于模拟传输），或者加上中继器以便将失真的数字信号进行整形（对于数字传输）。导线越粗，其通信距离就越远，但导线的价格也越高。在数字传输时，若传输速率为每秒几个兆比特，则传输距离可达几千米。由于双绞线的价格便宜且性能也不错，因此使用范围十分广泛。

为了提高双绞线的抗电磁干扰的能力，可以在双绞线的外面再加上一层用金属丝编织的屏蔽层，这就是屏蔽双绞线（Shielded Twisted Pair，STP）。它的价格当然比非屏蔽双绞线（Unshielded Twisted Pair，UTP）要贵一些。图1-30所示的是非屏蔽双绞线，图1-31所示的是屏蔽双绞线。

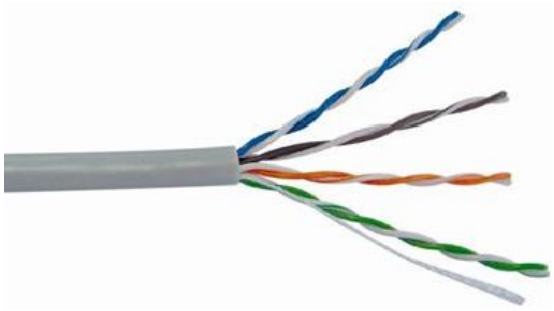


图1-30　非屏蔽双绞线



图1-31　屏蔽双绞线

1991年，美国电子工业协会（Electronic Industries Association，EIA）和电信行业协会（Telecommunications Industries Association，TIA）联合发布了一个标准EIA/TIA，它的名称是“商用建筑物电信布线标准”（Commercial Building Telecommunications Cabling Standard）。这个标准规定了用于室内传送数据的非屏蔽双绞线和屏蔽双绞线的标准。随着局域网上数据传送速率的不断提高，EIA/TIA也不断对其布线标准进行更新。

表1-1展示了常用的绞合线的类别、带宽和典型应用。无论是哪种类别的线，衰减都随频率的升高而增大。使用更粗的导线可以降低衰减，但却增加了导线的价格和重量；线对之间的绞合度（即单位长度内的绞合次数）和线对内两根导线的绞合度都必须经过精心设计，并在生产中加以严格的控制，使干扰在一定程度上得以抵消，这样才能提高线路的传输性能。使用更大的和更精确的绞合度可以获得更高的带宽。在设计布线时，要考虑受到衰减的信号应当有足够大的振幅，以便在有噪声干扰的条件下能够在接收端正确地被检测出来。双绞线究竟能够传送多高速率（Mbit/s）的数据还与数字信号的编码方法有很大的关系。

表1-1　常用的绞合线的类别、带宽和典型应用

绞合线类别	带　　宽	典 型 应 用
3	16MHz	低速网络；模拟电话

绞合线类别	带　　宽	典 型 应 用
4	20MHz	短距离的10BASE-T以太网
5	100MHz	10BASE-T以太网；某些100BASE-T快速以太网
5E（超5类）	100MHz	100BASE-T快速以太网；某些1000BASE-T吉比特以太网
6	250MHz	1000BASE-T吉比特以太网；ATM网络
7	600MHz	只使用STP，可用于10吉比特以太网

现在计算机连接使用的网线就是双绞线，其中有8根线，RJ-45连接头（俗称水晶头）的各触点对传输信号来说所起的作用分别是：1、2用于发送，3、6用于接收，4、5，7、8是双向线。对与其相连接的双绞线来说，为了降低相互干扰，要求1、2必须是绞缠的一对线，3、6也必须是绞缠的一对线，4、5相互绞缠，7、8相互绞缠。

8根线的接法标准分别为TIA/EIA 568B 和 TIA/EIA 568A。

TIA/EIA-568B：1、白橙，2、橙，3、白绿，4、蓝，5、白蓝，6、绿，7、白棕，8、棕。

TIA/EIA-568A：1、白绿，2、绿，3、白橙，4、蓝，5、白蓝，6、橙，7、白棕，8、棕。

如图1-32所示，网线的水晶头两端的线序如果都是T568B，我们称其为直通线；如果网线的一头的线序是T568B另一端是T568A，我们就称其为交叉线。不同的设备相连时要注意线序，不过现在网卡大多是自适应线序。

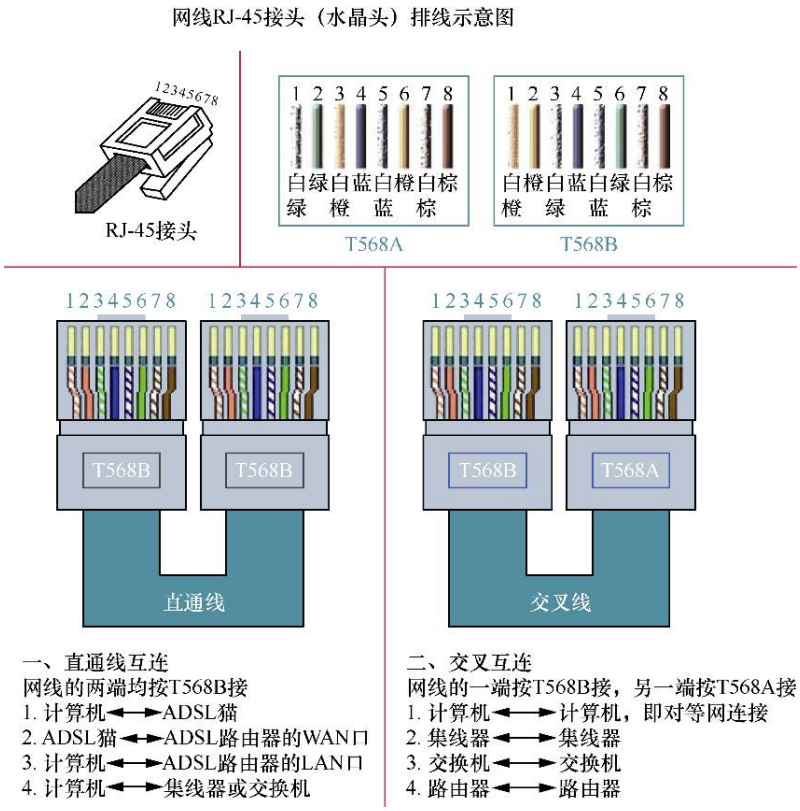


图1-32　线序

2. 同轴电缆

如图1-33所示，同轴电缆由内导体铜质芯线（单股实心线或多股绞合线）、绝缘层、网状的外导体屏蔽层（也可以是单股的）以及绝缘保护层（保护塑料外层）所组成。由于外导体屏蔽层的作用，所以同轴电缆具有很好的抗干扰特性，被广泛用于传输较高速率的数据。



图1-33　同轴电缆结构

在局域网发展的初期，我们曾广泛地使用同轴电缆作为传输媒体。但随着技术的进步，现在局域网领域基本上是采用双绞线作为传输媒体。目前同轴电缆主要用于有线电视网。同轴电缆的带宽取决于电缆的质量。目前高质量的同轴电缆的带宽已接近1GHz。

3．光缆

从20世纪70年代到现在，通信和计算机都发展得非常快。近20年来，计算机的运行速度大约每10年提高10倍。但在通信领域，信息的传输速率提高得更快，从20世纪70年代的56kbit/s提高到现在的几个到几十个Gbit/s（使用光纤通信技术），相当于每10年提高100倍。光纤通信成为了现代通信技术中的一个十分重要的领域。

光纤通信就是利用光导纤维（以下简称为光纤）传递光脉冲来进行通信。有光脉冲相当于1，没有光脉冲相当于0。由于可见光的频率非常高，约为10^8MHz的量级，因此一个光纤通信系统的传输带宽远远大于目前其他各种传输媒体的带宽。

光纤是光纤通信的传输媒体。当发送端有光源时，可以采用发光二极管或半导体激光器，它们在电脉冲的作用下能产生出光脉冲。在

接收端将光电二极管做成光检测器，在检测到光脉冲时可还原出电脉冲。

光纤通常是由非常透明的石英玻璃拉成细丝，它主要是由纤芯和包层构成的双层通信圆柱体。纤芯很细，其直径只有8μm～100μm（1μm=10^{6}m）。光波通过纤芯进行传导。包层较纤芯有较低的折射率。当光线从高折射率的媒体射向低折射率的媒体时，其折射角大于入射角（如图1-34所示）。因此，如果入射角足够大，就会出现全反射，即光线碰到包层时会折射回纤芯。这个过程不断重复，光也就沿着光纤传输下去。

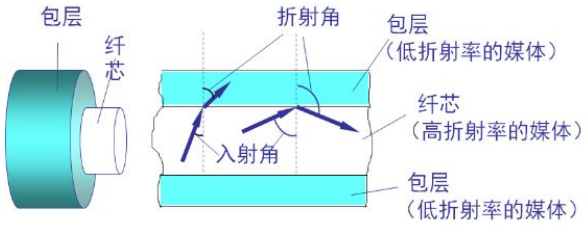


图1-34　光线在光纤中折射

图1-35是光波在纤芯中传播的示意图。现代的生产工艺可以制造出超低损耗的光纤，即做到光线在纤芯中传输数千米而几乎没有什么衰耗。这一点是光纤通信得到飞速发展的关键因素之一。

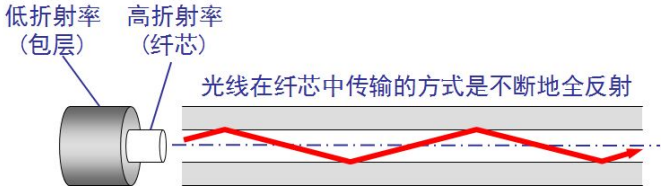


图1-35　光波在线芯中的传播

图1-35只画了一条光线。实际上，只要从纤芯中射到纤芯表面的光线的入射角大于某一个临界角度，就可产生全反射。因此，有许多条不同入射角度的光线会在一条光纤中传输。这种光纤就称为多模光纤（图1-36（a））。光脉冲在多模光纤中传输时会逐渐展宽，造成失真。因此多模光纤只适合于近距离传输。若光纤的直径减小到只有一个光的波长，则光纤就像一根波导那样，它可使光线一直向前传播，而不会产生多次反射。这样的光纤就称为单模光纤（图1-36（b））。单模光纤的纤芯很细，其直径只有几微米，制造起来成本较高。单模光纤的光源要使用昂贵的半导体激光器，而不能使用较便宜的发光二极管。但单模光纤的衰耗较小，在2.5Gbit/s的高速率下可传输数十千米而不必采用中继器。

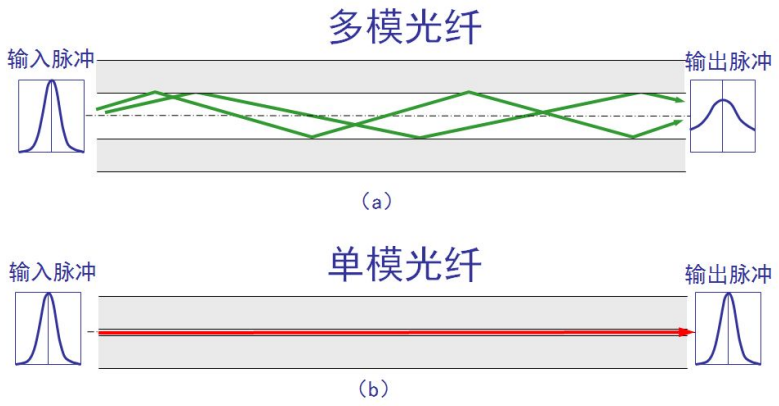


图1-36　单模光纤和多播光纤

光纤除了通信容量非常大的优点，还具有以下优点。

（1）传输损耗小，中继距离长，适用于远距离传输，经济实惠。

（2）抗雷电和电磁干扰性能好，这在有大电流脉冲干扰的环境下尤为重要。

（3）无串音干扰，保密性好，也不易被窃听或截取数据。

（4）体积小，重量轻。这在现有电缆管道已拥塞不堪的情况下特别有利。例如，1km长的1000对双绞线电缆约重8000kg，而同样长度但容量大得多的一对两芯光缆仅重100kg。

光纤也有一定的缺点，要将两根光纤精确地连接起来需要专用设备。

1.5.2　非导向传输媒体

前面介绍了3种导向传输媒体。但是，若通信线路要通过一些高山或岛屿，有时就很难施工。即使是在城市中，挖开马路铺设电缆也不是一件很容易的事。当通信距离很远时，铺设电缆既昂贵又费时。但利用无线电波在自由空间中的传播就可较快地实现多种通信。由于这种通信方式不使用之前介绍的各种导向传输媒体，因此称为“非导向传输媒体”。

特别要指出的是，由于信息技术的发展，社会各方面的节奏变快了。人们不仅要求能够在运动中进行电话通信（即移动电话通信），而且还要求能够在运动中进行计算机数据通信（俗称上网），现在的智能手机大多使用4G技术访问Internet。因此最近十几年无线电通信

发展得特别快，因为利用无线信道进行信息的传输，是在运动中通信的唯一手段。

1. 无线电频段

无线传输可使用的频段很广，人们现在已经利用了好几个波段进行通信。紫外线和更高的波段目前还不能用于通信。如图1-37所示，国际电信联盟（International Telecommunications Union，ITU）对不同波段取了正式名称。例如，LF波段的波长是从1km到10km（对应于30kHz到300kHz）。LF、MF和HF的中文名字分别是低频、中频和高频。更高的频段中的V、U、S和E分别对应于Very、Ultra、Super和Extremely，相应的频段的中文名字分别是甚高频、特高频、超高频和极高频。在低频LF的下面其实还有几个更低的频段，如甚低频VLF，特低频ULF，超低频SLF和极低频ELF等，因不用于一般的通信，故未在图中画出。

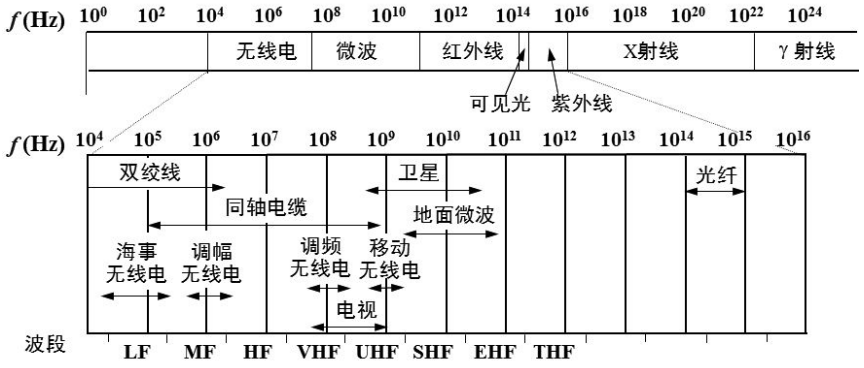


图1-37　电信领域使用的电磁波的频谱

表1-2列出了无线电波频段的名称和频段范围。

表1-2　无线电波划分

频段名称	频率范围	波段名称	波长范围
甚低频（VLF）	3kHz～30kHz	万米波，甚长波	10km～100km
低频（LF）	30kHz～300kHz	千米波，长波	1km～10km
中频（MF）	300kHz～3000kHz	百米波，中波	100m～1000m
高频（HF）	3MHz～30MHz	十米波，短波	10m～100m
甚高频（VHF）	30MHz～300MHz	米波，超短波	1m～10m
特高频（UHF）	300MHz～3000MHz	分米波	10cm～100cm
超高频（SHF）	3GHz～30GHz	厘米波	1cm～10cm
极高频（EHF）	30GHz～300GHz	毫米波	1mm～10mm

2. 短波通信

短波通信即高频通信，主要是靠电离层的反射。人们发现，当电波以一定的入射角到达电离层时，它也会像光学中的反射那样以相同的角度离开电离层。显然，电离层越高或电波进入电离层时与电离层

的夹角越小，电波从发射点经电离层反射到达地面的跨越距离越大，这就是利用电波可以进行远程通信的根本原因。而且，电波返回地面时又可能被大地反射而再次进入电离层，形成电离层的第二次、第三次反射，如图1-38所示。由于电离层对电波的反射作用，这就使本来是直线传播的电波有可能到达地球的背面或其他任何一个地方。电波经电离层的一次反射称为 “单跳”，单跳的跨越距离取决于电离层的高度。

但由电离层的不稳定所产生的衰落现象和电离层反射所产生的多径效应会使得短波信道的通信质量较差。因此，当必须使用短波无线电台传送数据时，一般都是低速传输，即速率为几十至几百比特/秒。只有在采用复杂的调制解调技术后，才能使数据的传输速率达到几千比特/秒。

3. 微波通信

微波通信在数据通信中占有重要地位。微波的频率范围为300MHz～300GHz（波长1mm～1m），但主要是使用2GHz～40GHz的频率范围。微波在空间主要是直线传播。由于微波会穿透电离层而进入宇宙空间，因此它不像短波那样可以经电离层反射传播到地面上很远的地方。传统的微波通信主要有两种主要的方式：即地面微波接力通信和卫星通信。

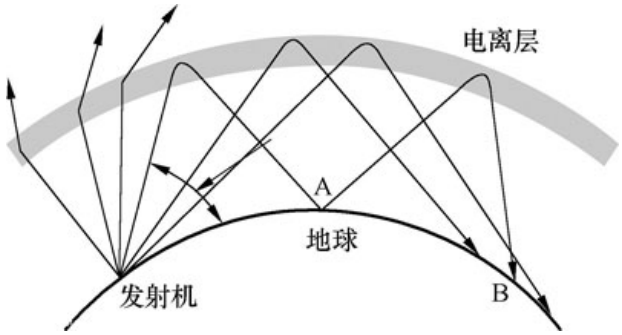


图1-38　短波通信

由于微波在空间是直线传播，而地球表面是个曲面，或地球上有高山或高楼等障碍，因此其传播距离受到限制，一般只有50km左右。但若采用100m高的天线塔，则传播距离可增大到100km。如图1-39所示，为实现远距离通信必须在一条无线电通信信道的两个终端之间建立若干个中继站。中继站把前一站送来的信号经过放大后再发送到下一站，故称为“接力”。

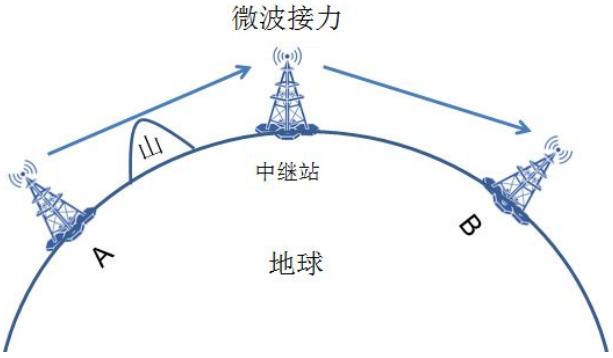


图1-39　微波接力通信

微波接力通信可传输电话、电报、图像、数据等信息。其主要特点如下所列。

（1）微波波段频率很高，其频段范围也很宽，因此其通信信道的容量很大。

（2）因为工业干扰和天电干扰的主要频谱成分比微波频率低得多，对微波通信的危害比对短波和米波（波长1m～10m的电磁波）通信小得多，因而微波传输质量较高。

（3）与相同容量和长度的电缆载波通信比较，微波接力通信建设投资少，见效快，易于跨越山区、江河。

当然，微波接力通信也存在如下的一些缺点。

（1）相邻站之间不能有障碍物。有时一个天线发射出的信号也会分成几条略有差别的路径到达接收天线，因而造成失真。

（2）微波的传播有时也会受到恶劣气候的影响。

（3）与电缆通信系统比较，微波通信的隐蔽性和保密性较差。

（4）大量中继站的使用和维护要耗费较多的人力和物力。

另一种微波中继是使用地球卫星，如图1-40所示。卫星通信方法是在地球站之间利用位于约3.6万千米高空的人造地球同步卫星作为中继器的一种微波接力通信。对地静止通信卫星就是在太空的无人值守的微波通信的中继站。可见卫星通信的主要优缺点应当大体上和地面微波通信的差不多。

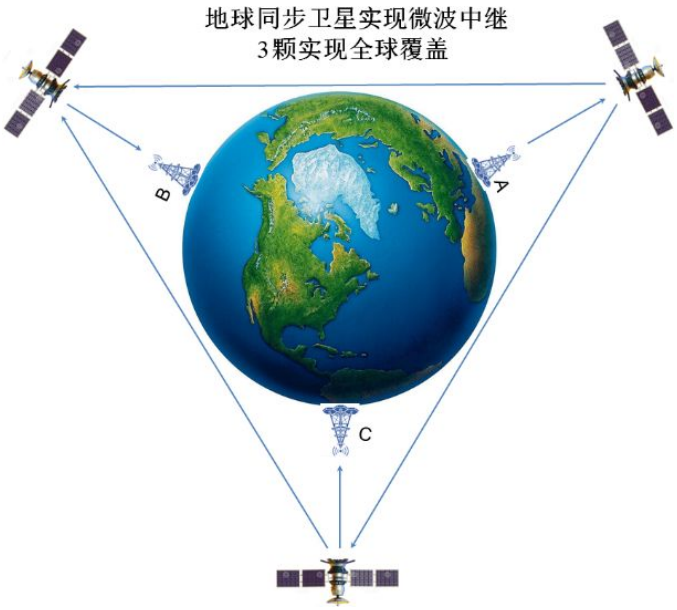


图1-40　短波通信使用卫星中继

卫星通信的最大特点是通信距离远，且通信费用与通信距离无关。地球同步卫星发射出的电磁波能辐射到地球上的通信覆盖区的跨度达 1.8 万多千米，面积约占全球的三分之一。在地球赤道上空的同步轨道上，如图1-40所示，放置 3 颗卫星，就能基本上实现全球的通信。和微波接力通信相似，卫星通信的频带很宽，通信容量很大，信号所受到的干扰也较小，通信比较稳定。为了避免产生干扰，赤道上空的卫星之间要有一定间隔，如果间隔不少于2度，那么整个赤道上空最多只能放置180颗同步卫星。好在人们想出来可以在卫星上使用不同的频段来进行通信。因此总的通信容量还是很大的。

卫星通信的另一特点就是具有较大的传播时延。由于各地球站的天线仰角并不相同，因此不管两个地球站之间的地面距离是多少（相隔一条街或相隔上万千米），从一个地球站经卫星到另一地球站的传播时延为250ms～300ms。一般可取为270ms。这和其他的通信有较大差

别（请注意：这和两个地球站之间的距离没有什么关系）。对比之下，地面微波接力通信链路的传播时延一般为3.3μs/km。

请注意，“卫星信道的传播时延较大”并不等于“用卫星信道传送数据的时延较大”。这是因为传送数据的总时延除了传播时延外，还有传输时延、处理时延和排队时延等部分。传播时延在总时延中所占的比例有多大，取决于具体情况。但利用卫星信道进行交互式的网上游戏显然是不合适的。卫星通信非常适合于广播通信，因为它的覆盖面很广。但从安全方面考虑，卫星通信系统的保密性是较差的。

4. 无线局域网

从20世纪90年代起，无线移动通信和因特网一样，得到了飞速的发展。与此同时，使用无线信道的计算机局域网也获得了越来越广泛的应用。我们知道，要使用某一段无线电频谱进行通信，通常必须得到本国政府有关无线电频谱管理机构的许可证。但是，也有一些无线电频段是可以自由使用的（只要不干扰他人在这个频段中的通信），这正好满足计算机无线局域网的需求。图1-41给出了美国的ISM频段，现在的无线局域网就使用其中的2.4GHz和5.8GHz频段。ISM是Industrial,Scientific,and Medical（工业、科学与医药）的缩写，即所谓的“工、科、医频段”。

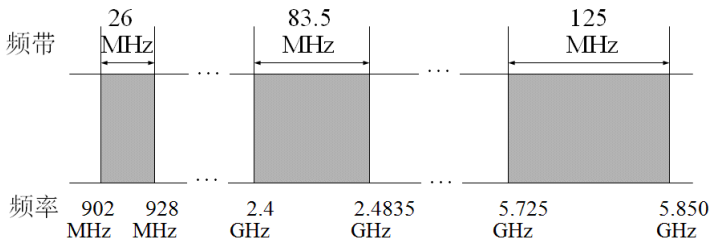


图1-41　无线局域网使用的ISM频段

1.6　网络分类

计算机网络按不同分类标准有多种类别。

1.6.1　按网络的范围进行分类

局域网（Local Area Network，LAN）是在一个局部的地理范围内（如一个学校、工厂和机关内），一般是方圆几千米以内，将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网。通常是单位自己采购设备组建局域网，当前使用交换机组建的局域网带宽为10Mbit/s、100Mbit/s或1000Mbit/s，无线局域网为54Mbit/s。

广域网（Wide Area Network，WAN）通常跨接很大的物理范围，所覆盖的范围从几十千米到几千千米，能连接多个城市或国家，甚至横跨几个洲来提供远距离通信，形成国际性的远程网络。比如某企业在北京和上海有两个局域网，把这两个局域网连接起来，就是广域网的一种。通常情况下广域网需要租用ISP（Internet服务提供商，比如电信、移动、联通公司）的线路，每年向ISP支付一定的费用购买带宽。带宽和支付的费用相关，就像你家用ADSL拨号访问Internet一样，有2Mbit/s带宽、4Mbit/s带宽、8Mbit/s带宽等标准。

城域网（Metropolitan Area Network，MAN）的作用范围一般是一个城市，可跨越几个街区甚至整个城市，其作用距离为5km～50km。城域网可以为一个或几个单位所拥有，也可以是一种公用设施，用来

将多个局域网进行互连。目前很多城域网采用的是以太网技术，因此有时也将其并入局域网的范围进行讨论。

个人区域网（Personal Area Network，PAN）就是在个人工作的地方把个人使用的电子设备（如便携式计算机等）用无线技术连接起来的网络，因此也常称为无线个人区域网（Wireless PAN，WPAN）。比如无线路由器组建的家庭网络，就是一个PAN，其范围大约在几十米。

1.6.2 按网络的使用者进行分类

网络按使用者分类，可分为公用网和专用网。这里讨论的网络特指计算机网络。

公用网（public network）是指电信公司（国有或私有）出资建造的大型网络。“公用”的意思就是所有愿意按电信公司的规定交纳费用的人都可以使用这种网络。因此公用网也称为公众网，因特网就是全球最大的公用网络。

专用网（private network）是某个机构为本单位的特殊业务工作需要而建造的网络。这种网络不向本单位以外的人提供服务。例如，铁路、电力等系统均有本系统的专用网。

1.7 习题

1．以太网交换机中的端口/MAC地址映射表（　　）。

A．是由交换机的生产厂商建立的

B．是交换机在数据转发过程中通过学习动态建立的

C．是由网络管理员建立的

D．是由网络用户利用特殊命令建立的

2．以太网使用什么协议在数据链路上发送数据帧（　　）。

A．HTTP

B．UDP

C．CSMA/CD

D．ARP

3．MAC地址通常存储在计算机的（　　）。

A．网卡的ROM中

B．内存中

C．硬盘中

D. 高速缓冲区中

4. 在Windows系统中查看网卡的MAC地址的命令是（　　）。

A. ipconfig /all

B. netstat

C. arp -a

D. ping

5. 关于交换机组网，以下哪些说法是错误的？（　　）

A. 交换机端口带宽独享，比集线器安全

B. 接口工作在全双工模式下，不再使用CSMA/CD协议

C. 能够隔绝广播

D. 接口可以工作在不同的速率下

6. 关于集线器，以下哪些说法是错误的？（　　）

A. 网络中的计算机共享带宽，不安全。

B. 使用集线器联网的计算机在一个冲突域中。

C. 接入集线器的设备需要有MAC地址，集线器基于帧的MAC地址转发。

D．使用CSMA/CD协议进行通信，每个接口带宽相同。

7．如图1-42所示，计算机C给计算机F发送一个帧，在图1-42中写出网桥1和网桥2在MAC地址表中增加的内容，MA、MB、MC、MD、ME和MF是计算机网卡的MAC地址。

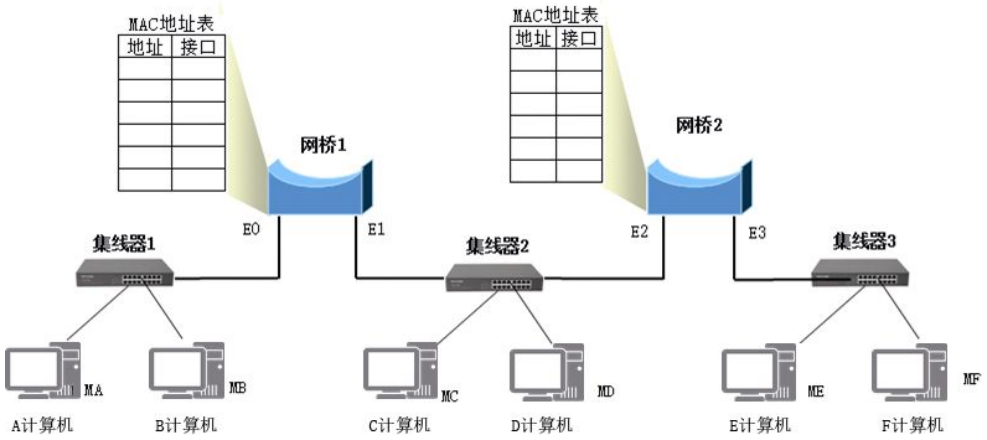


图1-42　构建MAC地址表

8．网卡的MAC地址在出厂时就已固化到ROM中，但是我们可以配置计算机不使用网卡ROM中的MAC地址，而使用指定的MAC地址。上网查资料，将你的计算机网卡的MAC地址加1，比如网卡的MAC地址是F4-8E-38-E7-37-83，更改为F4-8E-38-E7-37-84。

9．收发两端之间的传输距离为1000km，信号在媒体上的传播速率为2×10^8m/s。试计算以下两种情况的发送时延和传播时延。

（1）数据长度为10^7bit，数据发送速率为100kbit/s。

（2）数据长度为10^3bit，数据发送速率为1Gbit/s。

从以上计算结果可得出什么结论？

10．假设信号在媒体上的传播速率为2.3×10^8m/s。媒体长度分别为：

（1）10cm（网络接口卡）

（2）100m（局域网）

（3）100km（城域网）

（4）5000km（广域网）

试计算当数据率为1Mbit/s和10Gbit/s时信号在以上媒体中正在传播的比特数。

第2章　TCP/IP

本章内容

- 介绍TCP/IP
- 应用层协议
- 传输层协议
- 网络层协议
- 数据链路层协议
- 物理层协议
- OSI参考模型和TCP/IP

本章讲解计算机通信使用的TCP/IP及协议分层的标准和好处。

首先讲解什么是协议，签协议的意义和协议包含的内容。计算机通信使用的协议应该包含哪些约定，抓包分析应用层协议通信数据包，观察客户端发送请求和服务器端返回响应的交互过程，通过禁用应用层协议的特定方法限制客户端对服务器端的特定访问，实现高级安全控制。

然后讲解传输层协议TCP和UDP的应用场景，TCP协议实现可靠传输的机制，传输层协议和应用层协议之间的关系，服务和端口的关系，端口和网络安全的关系，随后展示如何设置Windows防火墙，关闭端口以实现网络安全。

最后讲解网络层协议、数据链路层协议和物理层协议，以及OSI参考模型和TCP/IP协议之间的关系。

2.1 介绍TCP/IP

学习计算机网络，最重要的就是掌握和理解计算机通信使用的协议。对很多学习计算机网络的人来说，协议是他们很不好理解的概念。因为计算机通信使用的协议，看不到摸不着，所以总是感觉非常抽象、难以想象。为此，在讲计算机通信使用的协议之前，先看一份租房协议，再去理解计算机通信使用的协议就不抽象了。

2.1.1 理解协议

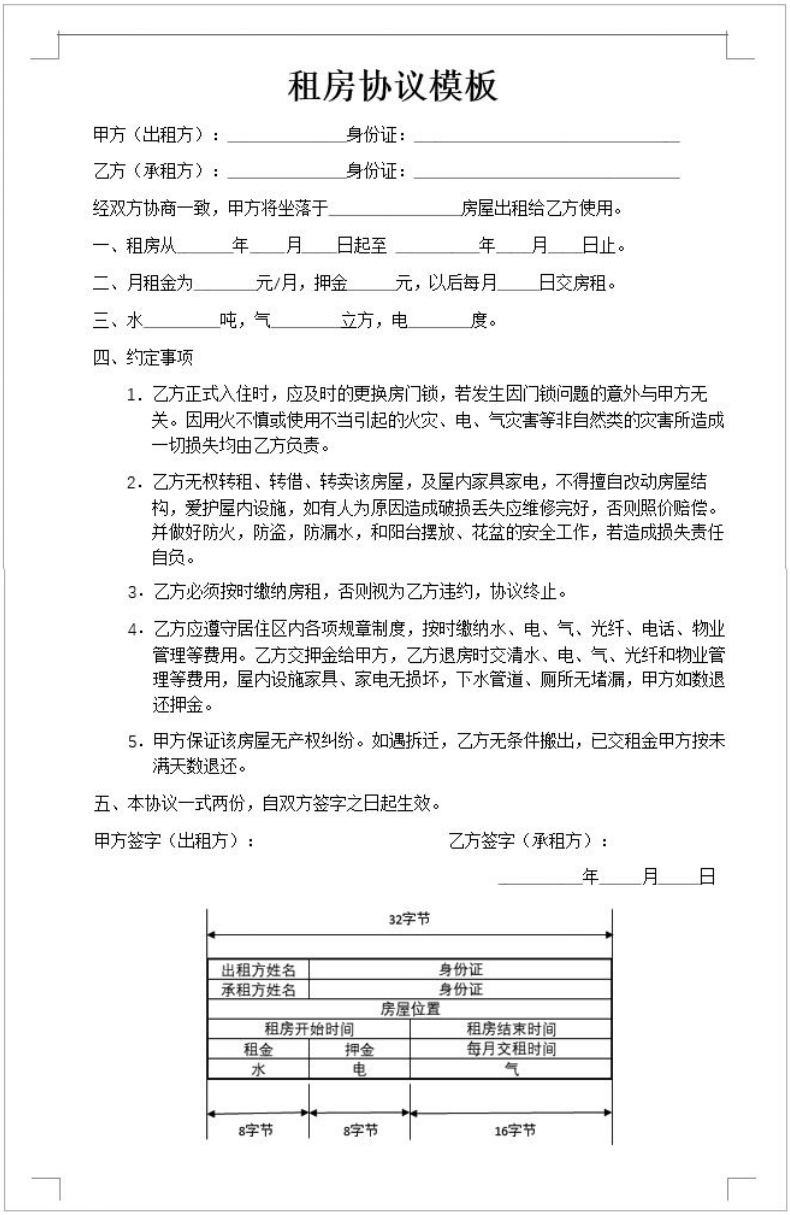
先来看一个租房协议，我们先理解协议的目的、要素，进而理解计算机通信使用的协议。

其实大家对于协议并不陌生，大学生走出校门参加工作就要和用人单位签署就业协议，工作后还有可能要租房住，就要和房东签署租房协议。下面就通过一个租房协议，来理解签协议的意义以及协议包含的内容，进而理解计算机通信使用的协议。

如果出租方和承租方不签协议，只是口头和出租方约定，房租多少、每个月几号交房租、押金多少、家具家电设施损坏谁负责。时间一长这些约定大家就都记不清了，一旦出现某种情况，承租方和出租方的认识不一致，就容易产生误解和矛盾。

为了避免纠纷，出租方和承租方就需要签一份租房协议，将双方关心的事情协商一致并写到协议中，双方确认后签字，协议一式两

份，双方都要遵守。签协议的双方有时候感觉会漏掉一些重要注意事项，于是就会从网上找一个公认的标准化的租房协议的模板。如图 2-1所示，它是一份租房协议模板，约定事项已经定义好，出租方和承租方只需按模板填写指定内容即可。



租房协议模板

甲方（出租方）：_____身份证：_____

乙方（承租方）：_____身份证：_____

经双方协商一致，甲方将坐落于_____房屋出租给乙方使用。

一、租房从_____年____月____日起至 _____年____月____日止。

二、月租金为_____元/月，押金_____元，以后每月____日交房租。

三、水_____吨，气_____立方，电_____度。

四、约定事项

1. 乙方正式入住时，应及时的更换房门锁，若发生因门锁问题的意外与甲方无关。因用火不慎或使用不当引起的火灾、电、气灾害等非自然类的灾害所造成一切损失均由乙方负责。
2. 乙方无权转租、转借、转卖该房屋，及屋内家具家电，不得擅自改动房屋结构，爱护屋内设施，如有人为原因造成破损丢失应维修完好，否则照价赔偿。并做好防火，防盗，防漏水，和阳台摆放、花盆的安全工作，若造成损失责任自负。
3. 乙方必须按时缴纳房租，否则视为乙方违约，协议终止。
4. 乙方应遵守居住区内各项规章制度，按时缴纳水、电、气、光纤、电话、物业管理等费用。乙方交押金给甲方，乙方退房时交清水、电、气、光纤和物业管理等费用，屋内设施家具、家电无损坏，下水管道、厕所无堵漏，甲方如数退还押金。
5. 甲方保证该房屋无产权纠纷。如遇拆迁，乙方无条件搬出，已交租金甲方按未满天数退还。

五、本协议一式两份，自双方签字之日起生效。

甲方签字（出租方）：　　乙方签字（承租方）：

_____年____月____日

图2-1　租房协议模板

为了简化协议填写，租房协议模板还定义了一个表格，如图2-2所示。出租房和承租方在签订租房协议时，只需将信息填写在表格规定的位置即可，协议的详细条款就不用再填写了。在表格中，出租方姓名、出租方身份证号、承租方姓名、承租方身份证号、房屋位置等称为字段，这些字段可以是定长，也可以是变长。如果是变长，那么要定义字段间的分界符。

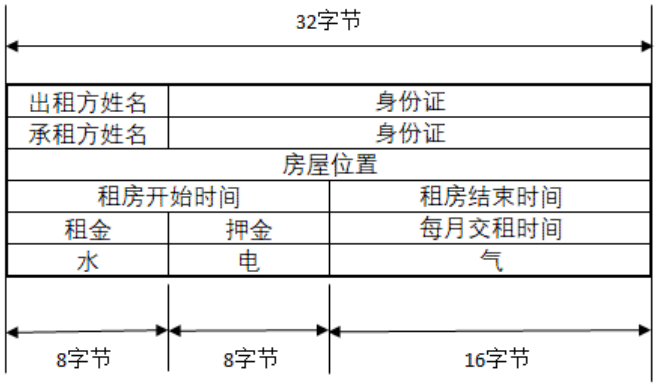


图2-2　租房协议模板定义的需要填写的表格

图2-3所示的是根据租房协议模板定义的表格所填写的一个具体的租房协议，根据该表格就知道出租房和承租方、房屋位置、租金、押金等信息，甲乙双方遵循的协议约定事项无须填写，但双方都知道租房协议模板的约定事项。

李华	XXXXXXXXXXXXXXXXXX	
韩梅梅	XXXXXXXXXXXXXXXXXX	
河北省石家庄塔谈小区12-1-22		
2019-11-01		2020-11-01
1400	1000	15日
122	1444	32

图2-3　具体的租房协议

计算机通信使用的协议也都进行了标准化，也就是形成了模板。像租房协议模板一样，计算机通信使用的协议有甲方和乙方，除了定义甲方和乙方遵循的约定外，它还会定义甲方和乙方交互信息时的报文格式。该格式通常包括请求报文和响应报文的格式，报文格式的定义如图2-2所示。在以后的学习中，如果使用抓包工具分析数据包，那么你看到的就是协议报文的各个字段，类似于图2-3中的租房协议中填写的各个字段。你看到的是每个字段的值，协议的具体条款看不到。图2-4所示的是IP定义的需要通信双方填写的表格，它叫作IP首部。网络中的计算机通信只需按着表格填写内容即可，这样通信双方的计算机和网络设备就能够按照IP的约定工作了。



图2-4　IP首部

应用程序通信使用的协议叫作应用层协议，应用层协议定义的需要填写的表格叫作报文格式。有的协议需要定义多种报文格式，比如ICMP，就有3种报文格式：ICMP请求报文、ICMP响应报文、ICMP差错报告报文。再比如HTTP，它定义了两种报文格式：HTTP请求报文、HTTP响应报文。

上面的租房协议是双方协议，协议中有甲、乙双方。有的协议是多方协议，比如大学生大四实习，要和实习单位签一份实习协议，实习协议就是三方协议：学生、学校和实习单位。协议规定了学生、学校以及实习单位需要遵循的约定。在很多计算机网络教材中，协议中的甲方和乙方被称为“对等实体”。

2.1.2 TCP/IPv4栈的分层

现在互联网中计算机通信使用的协议是TCP/IPv4协议栈，它是目前最完整、使用最广泛的通信协议之一。如图 2-5 所示，TCP/IPv4协议栈是一组协议，每一个协议都是独立的，有各自的甲方和乙方，有各自的目的和协议条款。这一组协议按功能分层，可分为应用层、传输层、网络层和数据链路层（网络接口层）。这一组协议共同工作才能实现网络中计算机之间的通信。

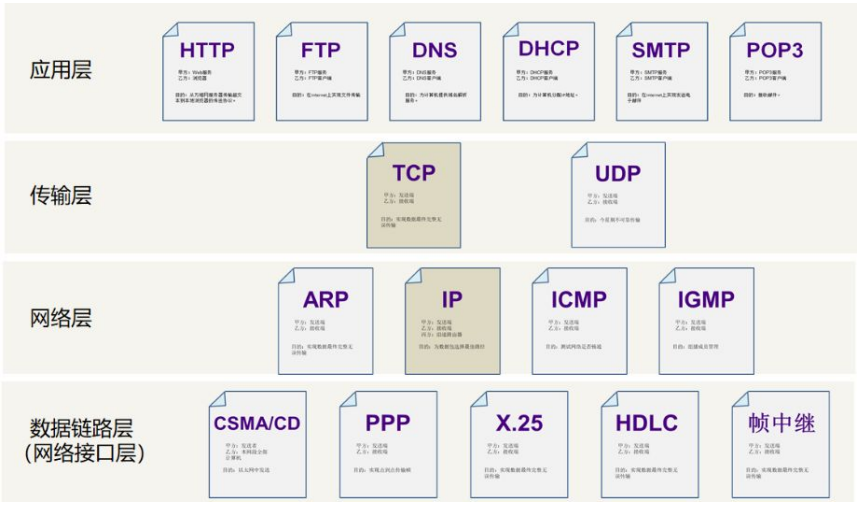


图2-5 TCP/IPv4协议栈

TCP/IPv4协议栈的魅力在于可使具有不同硬件结构、不同操作系统的计算机相互通信。TCP/IPv4协议栈既可用于广域网，也可用于局域网，它是Internet/Intranet 的基石。如图2-5所示，TCP/IPv4协议栈的主要协议有传输控制协议（TCP）和网际协议（IP）两个。

为什么说计算机通信需要这一组协议呢？怎么来理解分层呢？

大家想想网上购物，商家和顾客之间需要有购物协议，你也许没意识到这是购物协议，但商家和顾客在购物过程中一直按照购物平台要求的流程完成购物，顾客和商家的交互过程就相当于应用程序通信的交互过程，这是标准化的流程。商家提供商品，顾客浏览商品、选款式然后网上付款。接着商家发货，顾客收到货后确认收货，货款才能到商家账上，如果顾客不满意，还可以退货。购买了商品的顾客可以评价该商品。这就是购物需要的流程，可以认为是网络购物使用的协议。购物协议的甲方、乙方分别是商家和顾客，购物协议规定了购物流程、商家能做什么、顾客能做什么，操作顺序都定义好了。比如商家不能在付款前发货，顾客不能在未购物的情况下做出评价。这就相当于计算机通信使用的一个应用层协议。当然还有网上订餐，它也需要订餐流程，它相当于计算机通信中的另一个应用层协议。网络中的应用很多，比如访问网站、收发电子邮件、远程登录等，每一种应用都需要一个应用层协议。

只有购物协议就能实现网上购物了吗？购买的商品还需要快递到顾客家中，如果顾客不满意，可以将货品快递到商家。也就是说网上

购物还需要快递公司提供的物流功能。顺丰快递、圆通快递、中通快递等快递公司实现的是相同的功能：为网上购物提供物流服务。

快递公司投递快件，也需要有快递协议。快递协议规定了快件投送的流程以及投送快递需要填写的快递单。客户按着快递单的格式，在指定的地方填写收件人和发件人等信息。快递单规定了为了实现物流功能需要填写的表格，表格规定了要填写的内容。快递公司根据收件人所在的城市分拣快递，选择托运路线。快递到达目标城市后，快递人员根据快递单具体地址信息将快递投送给收件人。如图2-6所示，快递公司的快递单就相当于计算机通信中的网络层的IP所定义的IP首部，其目的就是把数据包发送到目标地址。



图2-6　快递单

快递公司为网上购物提供物流服务，类似的，TCP/IPv4协议栈分为4层，底层协议为它的上层协议提供服务，即传输层为应用层提供服务，网络层为传输层提供服务，数据链路层为网络层提供服务。

图2-7展示了TCP/IPv4协议栈的分层和作用范围。应用层协议的甲方和乙方分别是服务器端程序和客户端程序。传输层协议的甲方和乙

方分别是通信的两个计算机的传输层，TCP为应用层协议实现可靠传输，UDP为应用层协议提供报文转发。网络层协议中的IP为数据包跨网段转发选择路径。IP是多方协议，包括通信的两台计算机和沿途经过的路由器。路由器工作在网络层，网络层设备就是指路由器或三层交换机。数据链路层负责将网络层的数据包从链路的一端发送到另一端，数据链路层协议的作用范围是一段链路，不同的链路有不同的数据链路层协议。交换机负责将帧从一端发送到另一端，交换机属于数据链路层设备。

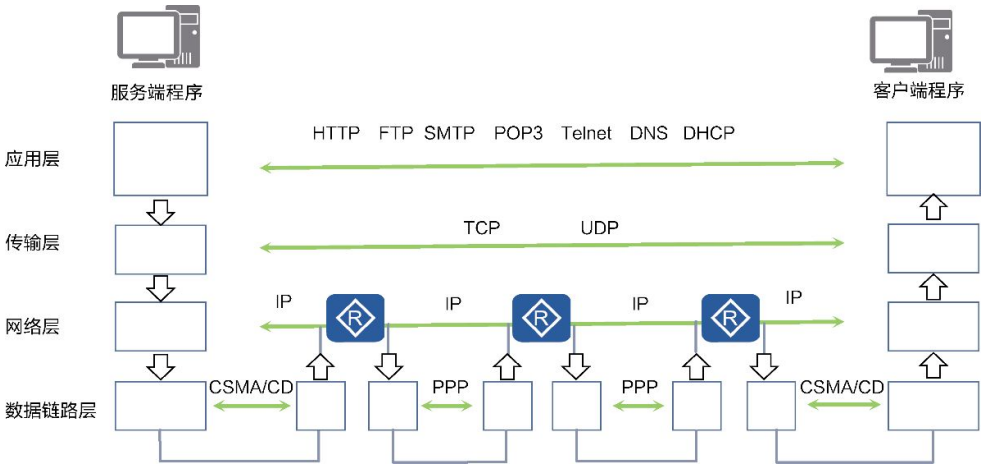


图2-7　协议的分层和作用范围

2.1.3　TCP/IPv4栈各层的功能

如图2-8所示，我们通常所说的TCP/IPv4栈不是一个协议，也不是TCP和IP两个协议，而是一组独立的协议。TCP/IPv4栈中的协议，按功能划分为4层，最高层是应用层，依次是传输层、网络层、网络接口层，本书将网络接口层拆分成两层来讲，即数据链路层和物理层。

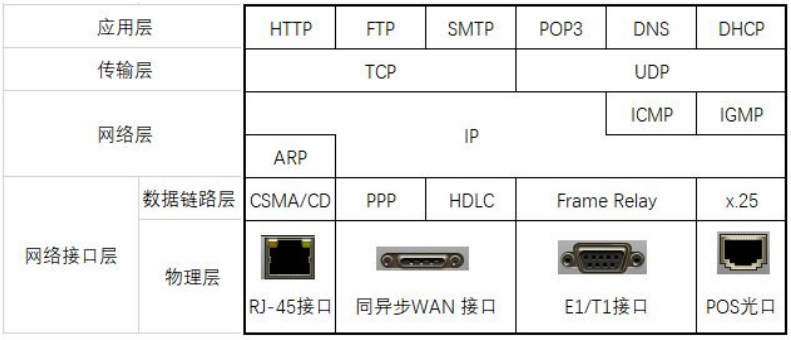


图2-8　TCP/IPv4栈分层

下面介绍各层实现的功能。

1. 应用层

应用层协议定义了互联网上常见的应用（服务器和客户端通信）通信规范。互联网中的应用很多，这就意味着应用层协议也很多，图2-8只列出了几个常见的应用层协议，但你不能认为就这几个。每个应用层协议定义了客户端能够向服务端发送哪些请求（也可以认为是哪些命令，这些命令发送的顺序），服务端能够向客户端返回哪些响应，这些请求报文和响应报文都有哪些字段，每个字段实现什么功能，每个字段的各种取值所代表的意思。

2. 传输层

传输层有两个协议，TCP和UDP。如果要传输的数据需要分成多个数据包发送，那么发送端和接收端的TCP要确保接收端最终完整无误地收到所传数据。如果在传输过程中网络出现丢包，那么发送端会超时

重传丢失的数据包。如果发送的数据包没有按发送顺序到达接收端，那么接收端会把数据包在缓存中排序，接着等待迟到的数据包，最终收到连续的、完整的数据。

UDP适用于应用层协议发送的内容用一个数据包就能发送完的场景，这种情况无须分段发送，不存在数据包是否按顺序到达的问题。数据发送是否成功，由应用程序判断。UDP要比TCP简单得多。

3. 网络层

网络层协议负责在不同网段间转发数据包，为数据包选择最佳的转发路径。网络中的路由器负责在不同网段转发数据包，为数据包选择转发路径，因此我们称路由器工作在网络层，是网络层设备。

4. 数据链路层

数据链路层协议负责把数据包从链路的一端发送到另一端。网络设备由网线或线缆连接，连接网络设备的这一段网线或线缆叫作一条链路。在不同的链路中传输数据有不同机制和方法，也就是有不同的数据链路层协议，比如以太网使用CSMA/CD协议，点到点链路使用PPP。

5. 物理层

物理层定义网络设备接口有关的一些特性，并对其进行标准化，比如接口的形状、尺寸、引脚数目和排列、固定和锁定装置、接口电缆的各条线上出现的电压范围等规定，这些都可以认为是物理层协议的内容。

协议按功能分层的好处就是，某一层的改变不会影响其他层。某层协议可以改进或改变，但它的功能是不变的。比如计算机通信可以使用IPv4也可以使用IPv6。网络层协议改变了，但其功能依然是为数据包选择转发路径，不会引起传输层协议的改变，也不会引起数据链路层的改变。

这些协议，每一层为上一层提供服务，物理层为数据链路层提供服务，数据链路层为网络层提供服务、网络层为传输层提供服务，传输层为应用层提供服务。以后网络出现故障，比如你不能访问Internet了，排除网络故障时要从底层到高层逐一检查。比如先看看网线是否连接，这是物理层排错；再ping Internet上的一个公网地址看看是否畅通，这是网络层排错；最后再检查浏览器设置是否正确，这是应用层排错。

2.1.4　封装和解封

如图2-9所示，商家给顾客发货，需要将“商品”打包，贴上快递单，这个过程可以叫作“封装”，封装后的快递包裹，我们称其为“快件”。顾客收到快件后，快递单就没用了，撕掉快递单打开包裹，看到购买的“商品”，这个过程可以叫作“解封”。快递员看不

到包裹中的商品，也不关心是什么商品，我们说快递员工作在物流层。当然商家和顾客也不关心包裹是走什么路线送达的，是空运还是铁路运输。类似的，计算机在通信过程也需要对要传输的数据进行封装和解封，封装后的数据有不同的名称。

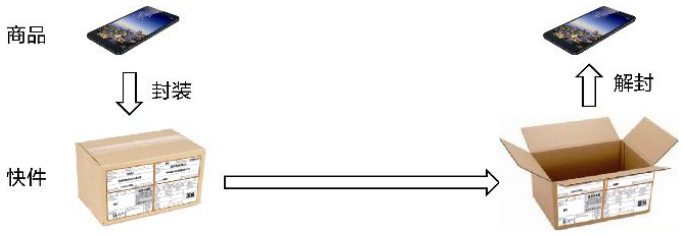


图2-9　封装和解封

如图2-10所示，应用程序通信需要发送的数据叫作“报文”，报文的格式由应用层协议定义。为了实现可靠传输，需要在传输层添加TCP首部，这就是“封装”，封装后就是“段”，TCP首部字段和格式由TCP协议定义。为了将数据段发送到目标计算机，需要在网络层为传输层的“段”添加IP首部，添加了IP首部的段称为“数据包”，IP首部字段和格式由IP定义。为了把数据包从链路的一端传输到另一端，需要给“数据包”添加数据链路层首部，以将数据包封装成“帧”。接收端收到后会去掉这些封装并提交给上层协议，这就是“解封”过程。

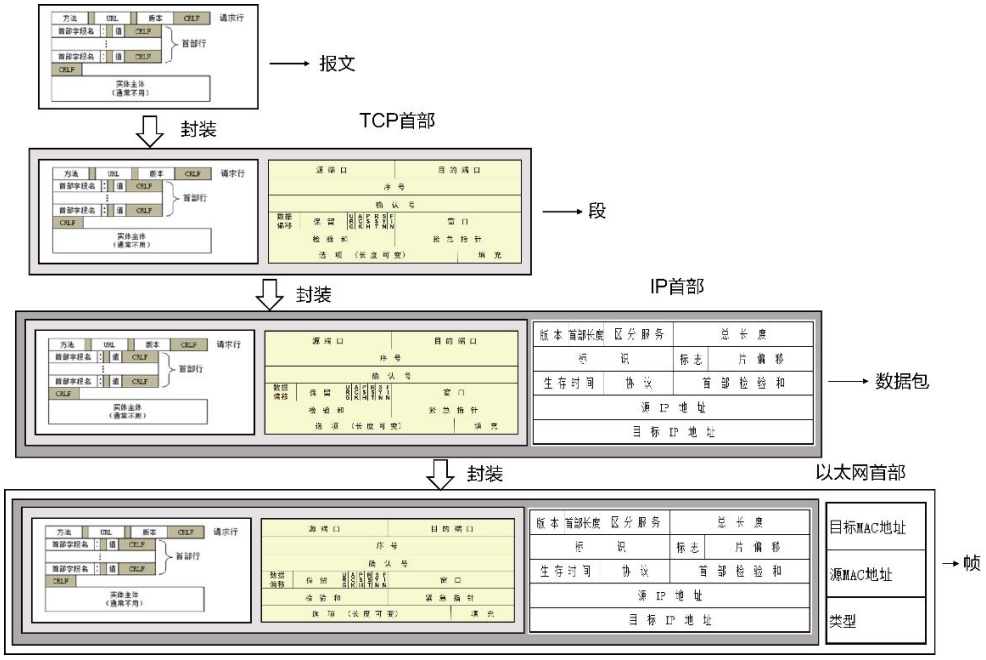


图2-10　封装

2.2　应用层协议

2.2.1　应用和应用层协议

网络中的计算机通信，实际上是计算机上的应用程序之间的通信，比如打开QQ和别人聊天，打开浏览器访问网站，打开暴风影音在线看电影，这些都会产生网络流量。

应用程序通常分为客户端程序和服务器端程序，客户端程序向服务器端程序发送请求，服务器端程序向客户端程序返回响应，提供服务。服务器端程序运行后等待客户端的连接请求。比如百度网站，不管是否有人访问百度网站，百度Web服务就一直等待客户端的访问请求，如图2-11所示。

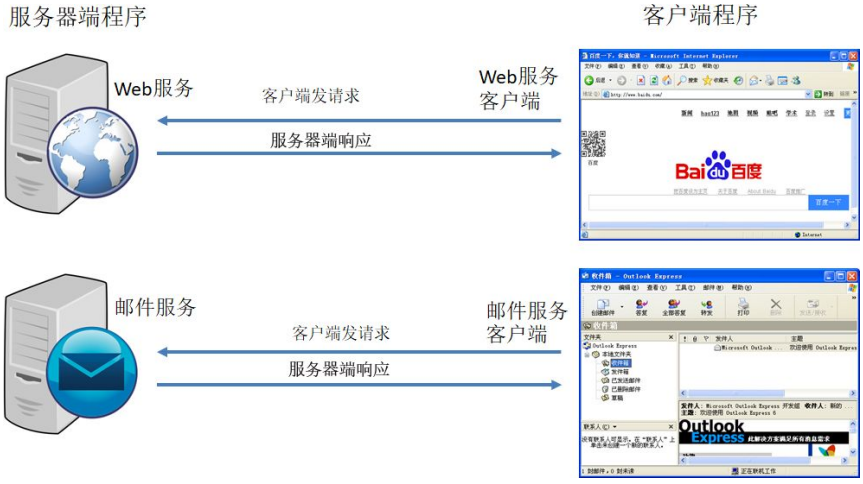


图2-11　客户端和服务器端程序通信

客户端程序能够向服务器端程序发送哪些请求，也就是客户端能够向服务器端发送哪些命令，这些命令发送的顺序，发送的请求报文有哪些字段，分别代表什么意思，都需要提前约定好。

服务器端程序收到客户端发来的请求。应该有哪些响应，什么情况发送什么响应，发送的响应报文有哪些字段，分别代表什么意思，也需要提前约定好。

这些提前约定好的客户端程序和服务器端程序通信规范就是应用程序通信使用的协议，称为应用层协议。Internet上有很多应用，比如访问网站的应用、收发电子邮件的应用、文件传输的应用、域名解析应用等，每一种应用都需要一个专门的应用层协议，这就意味着需要很多的应用层协议。

应用层协议的甲方和乙方是服务器端程序和客户端程序，在很多计算机网络原理的教材中，协议中的甲方和乙方称为对等实体。

2.2.2 应用层协议的标准化

TCP/IP是互联网通信的工业标准，TCP/IP中的应用层协议HTTP、FTP、SMTP、POP3都是标准化的应用层协议，应用层协议的标准化有什么好处呢？

Internet上用于通信的服务器端软件和客户端软件往往不是一家公司开发的，比如Web服务器有微软公司的IIS服务器，还有开放源代码的Apache、Nginx等，浏览器有微软的IE浏览器、UC浏览器、360浏

览器、火狐浏览器、谷歌浏览器等。你会发现Web服务器和浏览器虽然是不同公司开发的，但这些浏览器却能够访问全球所有的Web服务器，这是因为Web服务器和浏览器都是参照HTTP进行开发的，如图2-12所示。

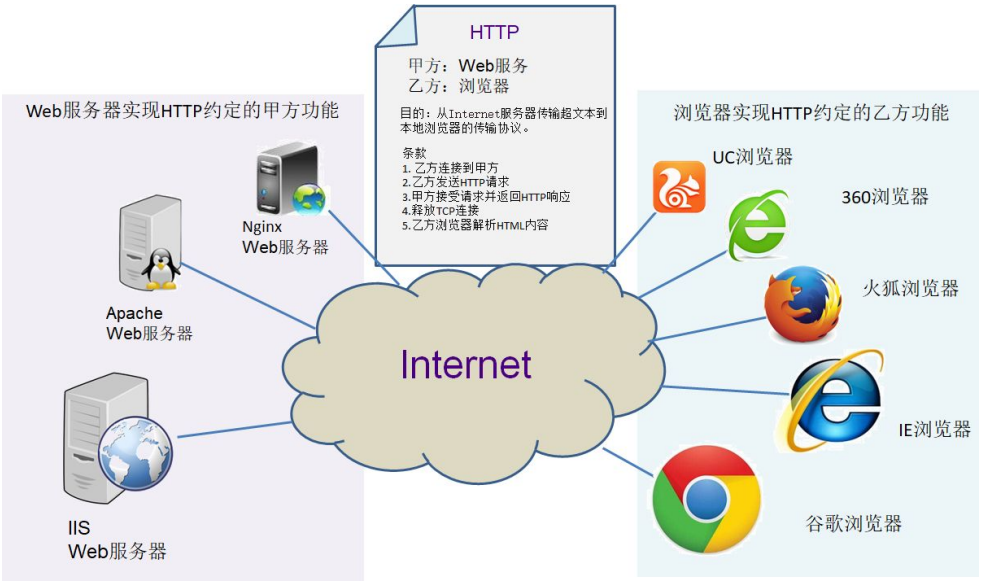


图2-12　HTTP使得各种浏览器能够访问各种Web服务器

HTTP定义了Web服务器和浏览器通信的方法，协议双方就是Web服务器和浏览器。为了更形象，我们称Web服务器为甲方、浏览器为乙方。

HTTP是TCP/IP中的一个标准协议，是一个开放式协议。由此你可以想到，肯定还有私有协议。比如在思科公司的路由器和交换机上运行的CDP（思科发现协议），只有思科的设备支持。比如你公司开发的一款软件有服务器端和客户端，它们之间的通信规范由开发者定义，这就是应用层协议。不过那些做软件开发的人如果不懂网络，没有学

过TCP/IP，那么他们并不会意识到他们定义的通信规范就是应用层协议，以及这样的协议就是私有协议，而这些私有协议不属于TCP/IP。

对于Internet上的常见应用，比如发送电子邮件、接收电子邮件、域名解析、文件传输、远程登录、地址自动配置等，它们通信使用的协议都已经成为Internet标准，并成为了TCP/IP中的应用层协议。下面列出了TCP/IP中常见的应用层协议。

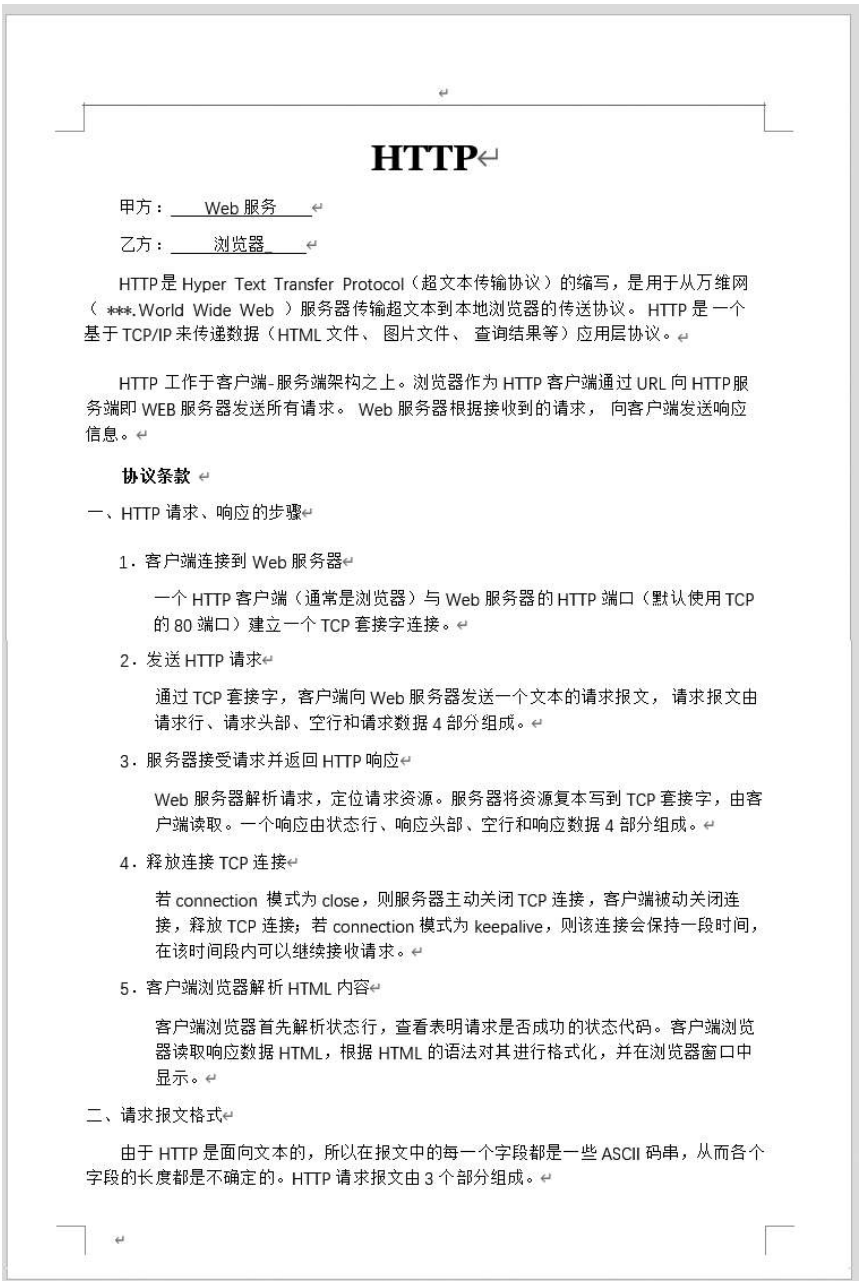
- 超文本传输协议：HTTP，用于访问Web服务器。
- 安全的超级文本传输协议：HTTPS，能够对HTTP协议通信进行加密访问。
- 简单邮件传输协议：SMTP，用于发送电子邮件。
- 邮局协议版本3：POP3协议，用于接收电子邮件。
- 域名解析协议：DNS协议，用于域名解析。
- 文件传输协议：FTP，用于上传和下载文件。
- 远程登录协议：Telnet协议，用于远程配置网络设备和Linux系统。
- 动态主机配置协议：DHCP，用于计算机自动请求IP地址。

2.2.3　以HTTP为例认识应用层协议

下面参照租房协议的格式将HTTP的主要内容列出来（注意：不是完整的），从而让读者更清楚地认识应用层协议，如图2-13所示。

可以看到HTTP定义了浏览器访问Web服务器的步骤，能够向Web服务器发送哪些请求（方法），HTTP请求报文格式（有哪些字段，分别

代表什么意思），也定义了Web服务器能够向浏览器发送哪些响应（状态码），HTTP响应报文格式（有哪些字段，分别代表什么意思）。



HTTP

甲方：Web 服务

乙方：浏览器

HTTP 是 Hyper Text Transfer Protocol（超文本传输协议）的缩写，是用于从万维网（ ***.World Wide Web ）服务器传输超文本到本地浏览器的传送协议。 HTTP 是一个基于 TCP/IP 来传递数据（HTML 文件、 图片文件、 查询结果等）应用层协议。

HTTP 工作于客户端-服务端架构之上。浏览器作为 HTTP 客户端通过 URL 向 HTTP 服务端即 WEB 服务器发送所有请求。 Web 服务器根据接收到的请求， 向客户端发送响应信息。

协议条款

一、HTTP 请求、响应的步骤

1．客户端连接到 Web 服务器

一个 HTTP 客户端（通常是浏览器）与 Web 服务器的 HTTP 端口（默认使用 TCP 的 80 端口）建立一个 TCP 套接字连接。

2．发送 HTTP 请求

通过 TCP 套接字，客户端向 Web 服务器发送一个文本的请求报文， 请求报文由请求行、请求头部、空行和请求数据 4 部分组成。

3．服务器接受请求并返回 HTTP 响应

Web 服务器解析请求，定位请求资源。服务器将资源复本写到 TCP 套接字，由客户端读取。一个响应由状态行、响应头部、空行和响应数据 4 部分组成。

4．释放连接 TCP 连接

若 connection 模式为 close，则服务器主动关闭 TCP 连接，客户端被动关闭连接，释放 TCP 连接；若 connection 模式为 keepalive，则该连接会保持一段时间，在该时间段内可以继续接收请求。

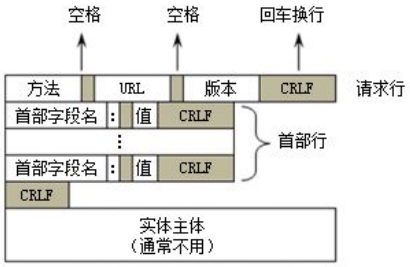
5．客户端浏览器解析 HTML 内容

客户端浏览器首先解析状态行，查看表明请求是否成功的状态代码。客户端浏览器读取响应数据 HTML，根据 HTML 的语法对其进行格式化，并在浏览器窗口中显示。

二、请求报文格式

由于 HTTP 是面向文本的，所以在报文中的每一个字段都是一些 ASCII 码串，从而各个字段的长度都是不确定的。HTTP 请求报文由 3 个部分组成。

图2-13　HTTP



1．开始行

用于区分是请求报文还是响应报文。请求报文中的开始行叫作请求行，而响应报文中的开始行叫作状态行。在开始行的3个字段之间都以空格分隔开，最后的“CR”和“LF”分别代表“回车”和“换行”。

2．首部行

用来说明浏览器、服务器或报文主体的一些信息。首部可以有好几行，但也可以不使用。在每一个首部行中都有首部字段名和它的值，每一行在结束的地方都要有“回车”和“换行”。整个首部行结束时，还有一空行将首部行和后面的实体主体分开。

3．实体主体

请求报文中一般都不用这个字段，而响应报文中也可能没有这个字段。

三、HTTP请求报文中的方法

浏览器能够向Web服务器发送以下8种方法（有时也叫“动作”）来表明对URL指定的资源的不同操作方式。

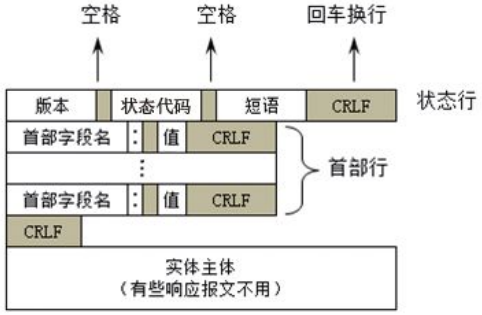
- GET：请求获取URL所标识的资源。使用在浏览器的地址栏中输入网址的方式访问网页时，浏览器采用GET方法向服务器请求网页。
- POST：在URL所标识的资源后附加新的数据。要求被请求服务器接收附在请求后面的数据，常用于提交表单，比如向服务器提交信息、发帖、登录。
- HEAD：请求获取由URL所标识的资源的响应消息报头。
- PUT：请求服务器存储一个资源，并用URL作为其标识。
- DELETE：请求服务器删除URL所标识的资源。
- TRACE：请求服务器回送收到的请求信息，主要用于测试或诊断。
- CONNECT：用于代理服务器。
- OPTIONS：请求查询服务器的性能，或者查询与资源相关的选项和需求。

图2-13　HTTP（续）

方法名称是区分大小写的。当某个请求所针对的资源不支持对应的请求方法的时候，服务器应当返回状态代码 405（Method Not Allowed）；当服务器不认识或者不支持对应的请求方法的时候，应当返回状态代码 501（Not Implemented）。

四、响应报文格式

每一个请求报文发出后，都能收到一个响应报文。响应报文的第一行就是状态行。状态行包括3 项内容，即 HTTP 的版本、状态代码，以及解释状态代码的简单短语，如下所示。



五、HTTP 响应报文状态码

状态代码（Status-Code）都是 3 位数字的，分为 5 大类共 33 种，例如：

- 1xx 表示通知信息，如请求收到了或正在进行处理；
- 2xx 表示成功，如接收或知道了；
- 3xx 表示重定向，如要完成请求还必须采取进一步的行动；
- 4xx 表示客户端错误，如请求中有错误的语法或不能完成；
- 5xx 表示服务器出现差错，如服务器失效无法完成请求。

下面几种状态行在响应报文中是经常见到的。

HTTP/1.1 202 Accepted （接收）

HTTP/1.1 400 Bad Request （错误的请求）

HTTP/1.1 404 Not Found （找不到）

图2-13 HTTP（续）

举一反三，其他的应用层协议也需要定义以下内容。

- 客户端能够向服务器发送哪些请求（方法或命令）。

- 客户端和服务器命令的交互顺序，比如POP3协议，需要先验证用户身份才能收邮件。
- 服务器有哪些响应（状态代码），每种状态代码代表什么意思。
- 定义协议中每种报文的格式：有哪些字段，字段是定长还是变长，如果是变长，字段分割符是什么，这些都要在协议中定义。一个协议有可能需要定义多种报文格式，比如ICMP协议定义了ICMP请求报文格式、ICMP响应报文格式和ICMP差错报告报文格式。

2.2.4 抓包分析应用层协议

在计算机中安装抓包工具可以捕获网卡发出和接收到的数据包，还能够捕获应用程序通信的数据包。这样就可以直观地看到客户端和服务器端的交互过程，如客户端发送了哪些请求，服务器返回了哪些响应等。这些也是应用层协议的工作过程。

接下来介绍使用抓包工具捕获SMTP客户端（Outlook Express）向SMTP服务器端发送电子邮件的过程，我们可以看到客户端向服务器发送的请求（命令）以及服务器向客户端发送的响应（状态代码）。

抓包工具Ethereal有两个版本，在Windows XP和Windows Server 2003上使用Ethereal抓包工具，在Windows 7和Windows 10上使用Wireshark（Ethereal的升级版）抓包工具。建议在VMWare Workstation虚拟机中完成抓包分析过程。以下操作在Windows XP虚拟机中进行。因为Windows XP中有Outlook Express，所以将虚拟机网卡

指定到NAT网络后，抓包工具就不会捕获物理网络中大量无关的数据包了。

登录网易邮箱的网站，申请一个电子邮箱，然后启用POP3和SMTP服务，如图2-14所示。

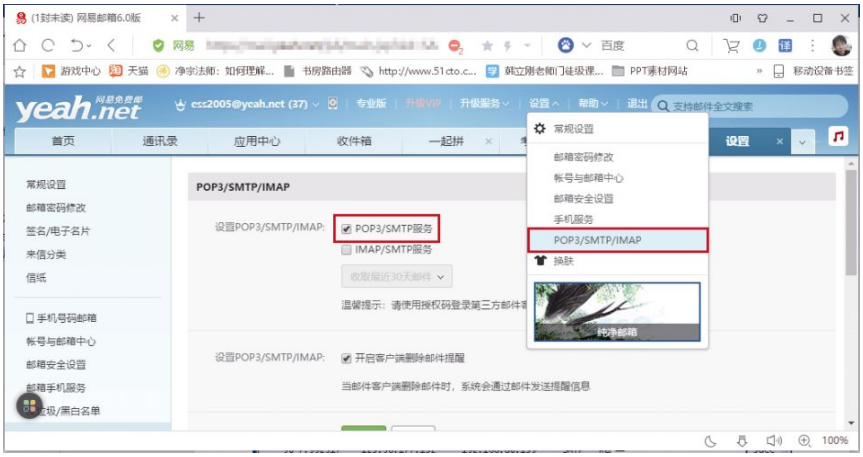


图2-14　启用POP3和SMTP服务

在Windows XP上安装Ethereal，然后运行抓包工具。再打开Outlook Express，将申请的电子邮件账户连接到邮件服务器，给自己写一封邮件，单击“发送/接收”，停止抓包。如图2-15所示，可以看到发送邮件的协议SMTP，右键单击该数据包，并单击Follow TCP Stream。

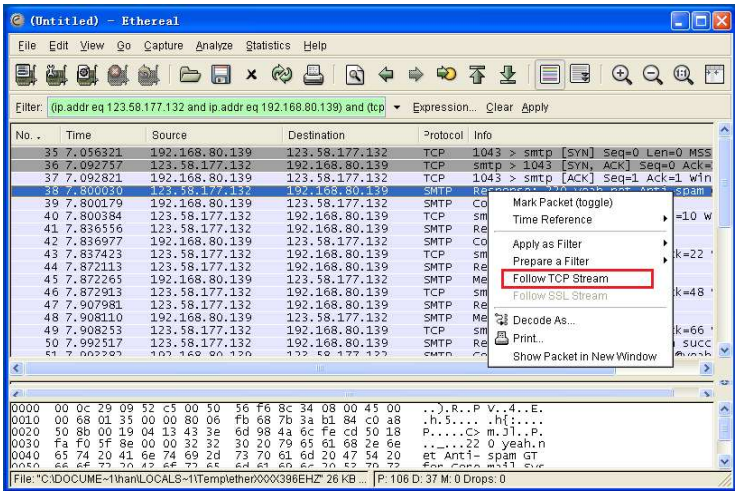


图2-15　筛选数据包

Outlook Express就是SMTP客户端，如图2-16所示，可以看到SMTP客户端向SMTP服务器发送电子邮件的交互过程。

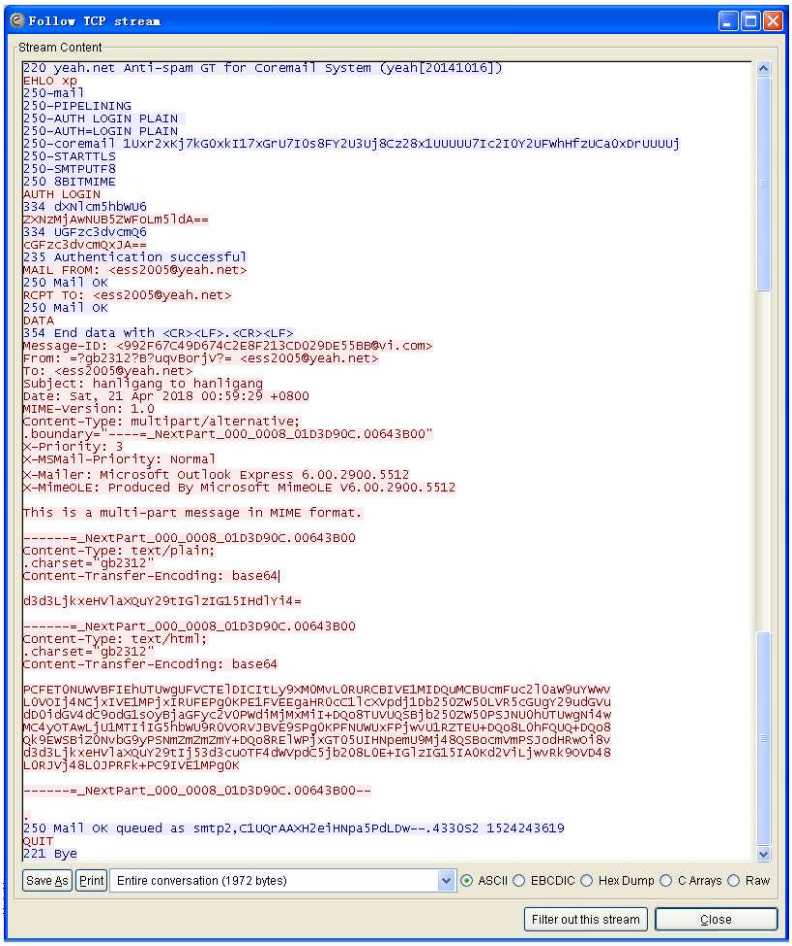


图2-16　发送电子邮件的交互过程

图2-16中SMTP客户端向SMTP服务器发送的命令以及顺序如下。

EHLO xp 证，xp是客户端计算机名	--EHLO是对HELO的扩展，可以支持用户认
AUTH LOGIN	--需要身份验证
MAIL FROM: <ess2005@yeah.net>	--发件人
RCPT TO: <ess2005@yeah.net>	--收件人
DATA	--邮件内容
.	--表示结束，将输入内容一起发送出去
QUIT	--退出

图2-16中有状态代码的行是SMTP服务器向SMTP客户端返回的响应。

```
220<domain>        --服务器就绪
250                --要求的邮件操作完成
334                --服务器响应，已经过BASE64编码的用户名和密码
354                --开始邮件输入，以"."结束
221                --服务关闭
```

从以上捕获到的数据包中，我们可以看到SMTP、客户端向服务器发送的命令以及服务器返回的响应。

2.2.5 应用层协议和高级防火墙

高级防火墙能够识别应用层协议的方法，我们可以设置高级防火墙来禁止客户端向服务器发送某个请求，也就是禁用应用层协议的某个方法。比如浏览器请求网页使用的是GET方法，向Web服务器提交内容使用的是POST方法。如果企业不允许员工在Internet上的论坛发帖，那么可以在企业网络边缘部署高级防火墙以禁止HTTP的POST方法，如图2-17所示。

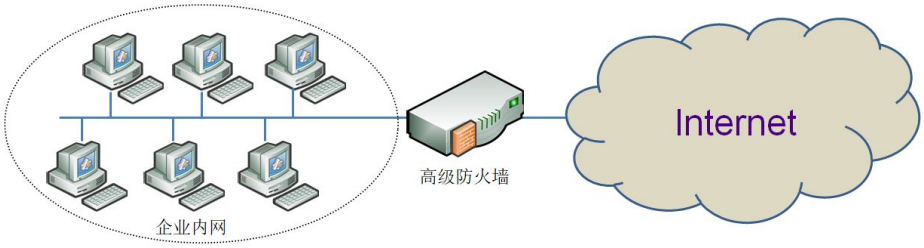


图2-17 部署高级防火墙

图2-18所示的是微软企业级防火墙TMG，配置HTTP以阻止POST方法。注意：方法名称区分大小写。

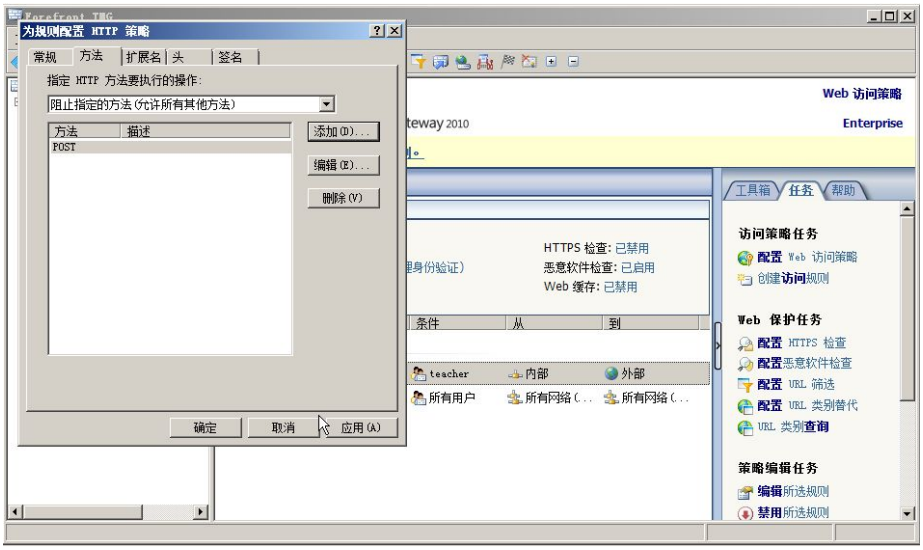


图2-18　阻止HTTP的POST方法

在Windows Server 2012 R2上安装FTP服务，可以禁止FTP的某些方法。下面的操作就是在Windows 7中安装Wireshark抓包工具；开始抓包后，访问Windows Server 2012 R2上的FTP服务；然后上传一个test.txt文件，并将其重命名为abc.txt；最后删除FTP服务器上的abc.txt文件，这样抓包工具会捕获FTP客户端发送的全部命令。

如图2-19所示，右键单击某个FTP协议数据包，然后单击“追踪流”“TCP流”。

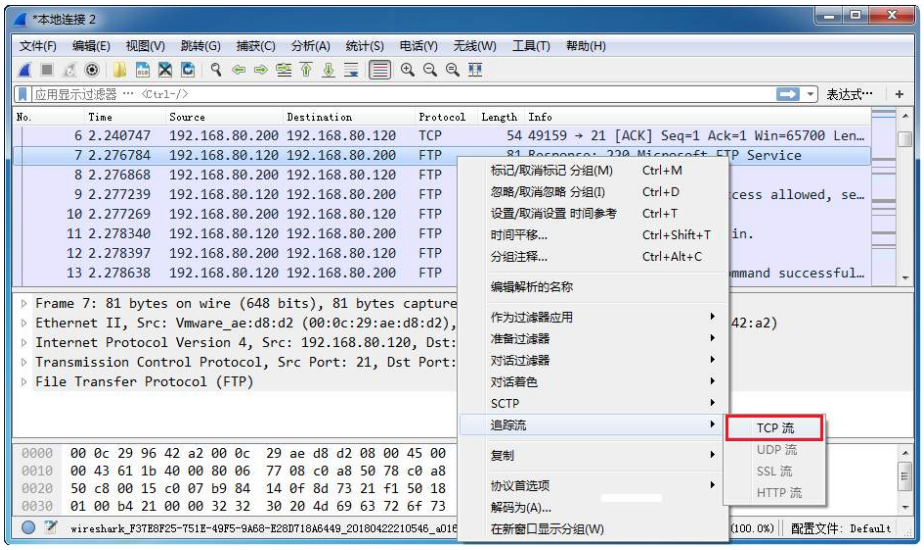


图2-19　访问FTP服务器的数据包

接下来会出现图2-20所示的窗口，它将FTP客户端访问FTP服务器的所有交互过程中产生的数据整理到了一起。我们可以从中看到FTP中的方法，“STOR”方法上传test.txt，“CWD”方法改变工作目录，“RNFR”方法重命名test.txt，“DELE”方法删除abc.txt文件。如果想看到FTP的其他方法，可以使用FTP客户端在FTP服务器上执行创建文件夹、删除文件夹、下载文件等操作，这些操作对应的方法使用抓包工具都能看到。

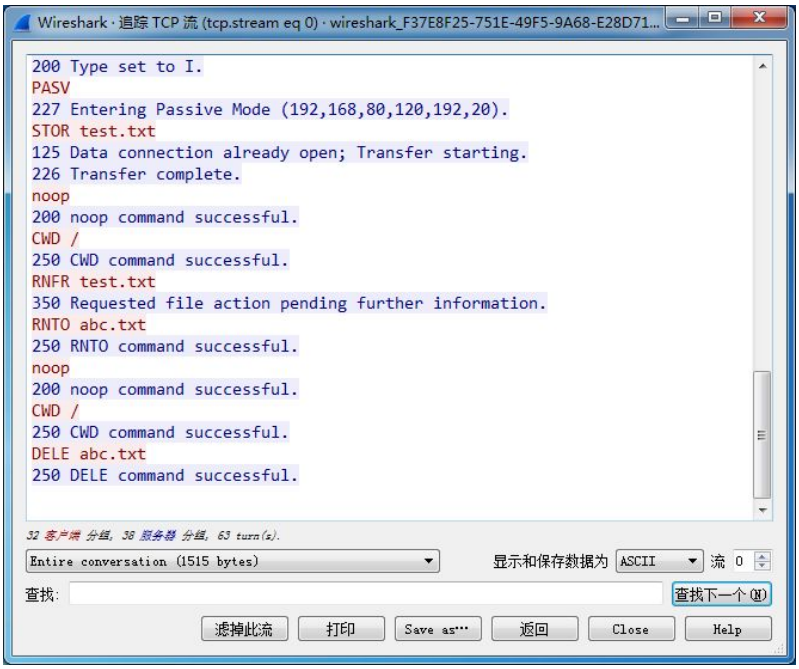


图2-20　FTP客户端访问FTP服务器的交互过程

我们也可以配置FTP服务器以禁止FTP中的一些方法。比如想要禁止FTP客户端删除FTP服务器上的文件，那么可以配置FTP请求筛选，从而禁止DELE方法。如图2-21所示，单击“FTP请求筛选”。

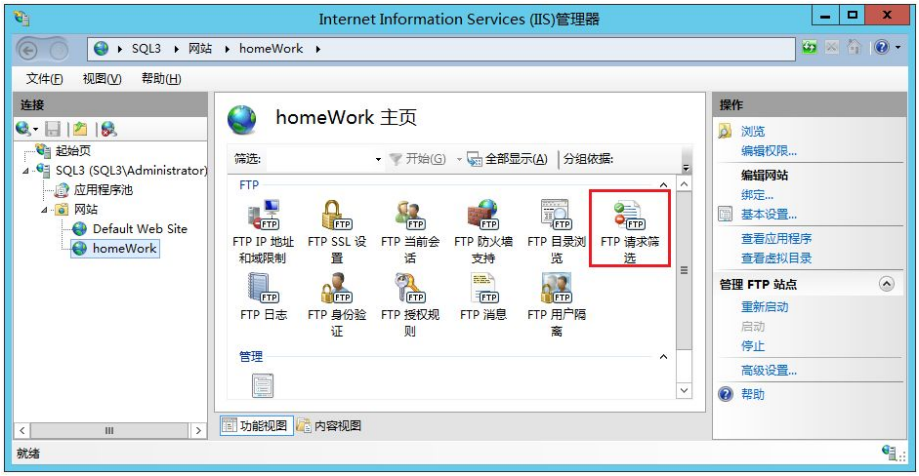


图2-21　配置FTP请求筛选

如图2-22所示，在“FTP请求筛选”界面中单击“命令”标签，然后单击“拒绝命令…”，在出现的“拒绝命令”对话框中输入“DELE”，单击“确定”按钮。

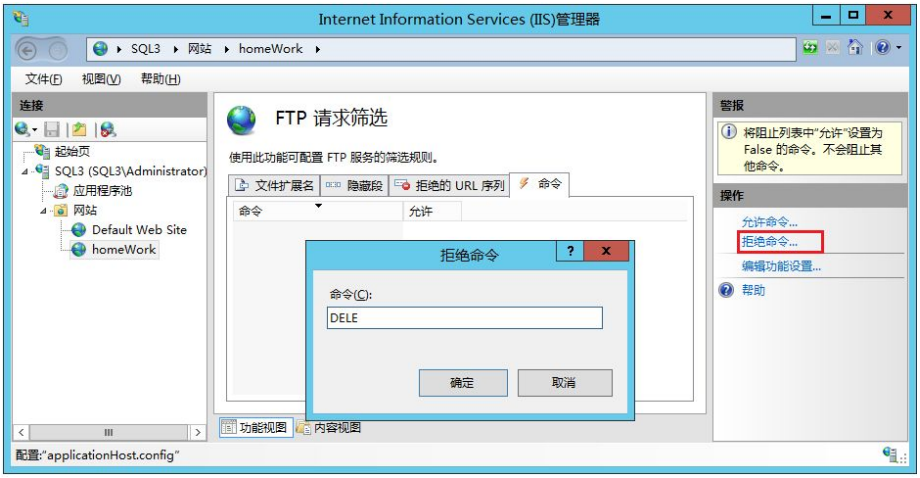


图2-22　禁用DELE方法

此时再在Windows 7上删除FTP服务器上的文件时，就会出现提示“500 Command not allowed.”，如图2-23所示，意为命令不被允许。



图2-23　命令不允许

Windows Server 2012 R2的Web站点也可以禁止HTTP的某些方法，如图2-24所示，单击“请求筛选”。



图2-24　筛选HTTP协议请求

如图2-25所示，在“HTTP谓词”标签下，单击“拒绝谓词…”，输入拒绝的方法“POST”，此时浏览器向该网站发送的POST请求就被拒绝。



图2-25　禁用HTTP的“POST”方法

2.3 传输层协议

2.3.1 TCP和UDP的应用场景

传输层的两个协议，传输控制协议（Transmission Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）有各自的应用场景。

TCP为应用层协议提供可靠传输，发送端按顺序发送，接收端按顺序接收。其间若出现丢包、乱序现象，TCP负责重传和排序。下面是TCP的应用场景。

（1）客户端程序和服务端程序需要多次交互才能实现应用程序的功能，比如接收电子邮件使用的POP3和发送电子邮件的SMTP，以及传输文件的FTP，都需要客户端程序和服务端程序多次交互。

（2）应用程序传输的文件需要分段传输。比如浏览器访问网页，网页中图片和HTML文件需要分段后发送给浏览器，或QQ传文件，这些场景在传输层选用的是TCP。

如果需要将发送的内容分成多个数据包发送，这就要求在传输层使用TCP，并在发送方和接收方建立连接，从而实现可靠传输、流量控制和拥塞避免。

比如从网络中下载一个500MBit的电影或下载一个200MBit的软件，这么大的文件需要拆分成多个数据包发送，发送过程需要持续几分钟或几十分钟。在此期间，发送方将要发送的内容一边发送一边放到缓存，将缓存中的内容分成多个数据包并进行编号，然后按顺序发送。这就需要在发送方和接收方之间建立连接，协商通信过程的一些参数（比如一个数据包最大有多少字节），如果网络不稳定造成某个数据包丢失，那么发送方必须重新发送丢失的数据包，否则就会造成接收到的文件不完整，这就需要TCP来实现可靠传输。如果发送方发送速度太快，接收方来不及处理，接收方会通知发送方降低发送速度甚至停止发送。TCP还能实现流量控制。互联网中的流量不固定，流量过高时会造成网络拥塞（这一点很好理解，就像城市上下班高峰时的交通堵塞一样），在整个传输过程中发送方要一直探测网络是否拥塞来调整发送速度。TCP有拥塞避免机制。

如图2-26所示，发送方的发送速度由网络是否拥塞和接收端接收速度两个因素控制，哪个速度低，就用哪个速度发送。

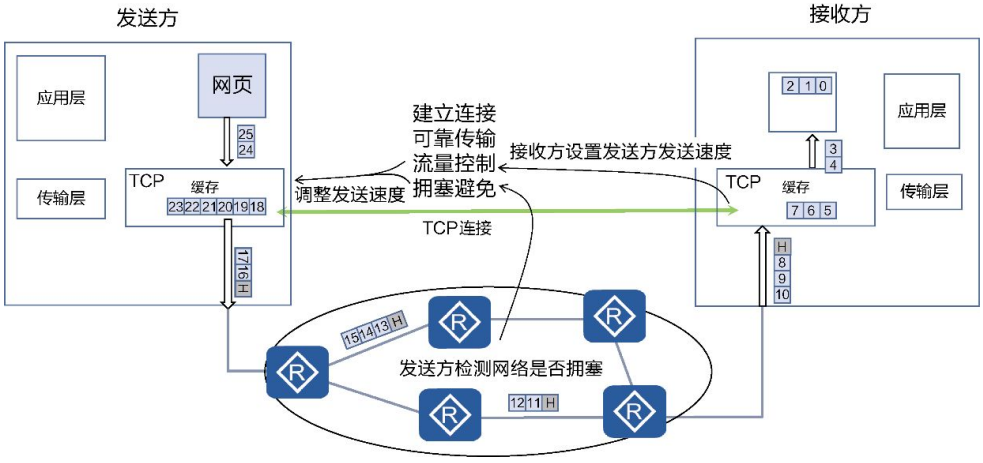


图2-26　TCP功能

在有些应用程序通信中，使用TCP就会降低效率。比如有些应用，客户端只需向服务器发送一个请求报文，服务器返回一个响应报文就实现其功能。这类应用如果使用TCP，发送3个数据包建立连接，再发送4个数据包释放连接，就为了发送一个报文，就显得不值了。干脆让应用程序直接发送，如果丢包了，应用程序再发送一遍。面对这类应用，在传输层就使用UDP。

UDP的应用场景如下。

（1）客户端程序和服务端程序通信时，应用程序发送的数据包不需要分段。比如域名解析，DNS协议就是用传输层的UDP，客户端向DNS服务器发送一个报文以解析某个网站的域名，DNS服务器将解析的结果使用一个报文返回给客户端。

（2）实时通信，比如QQ语音聊天、微信语音聊天或视频聊天。在这类应用中，发送端和接收端需要实时交互，也就是不允许较长延迟，即便有几句话因为网络堵塞没听清，也不允许使用TCP等待丢失的报文。等待的时间太长了，就不能愉快地聊天了。

（3）多播或广播通信。比如学校多媒体机房，老师的计算机屏幕需要教室的学生计算机接收，在老师的计算机上安装多媒体教室服务端软件，在学生计算机上安装多媒体教室客户端软件，老师计算机使用多播地址或广播地址发送报文，学生计算机都能收到。这类应用在传输层使用UDP。

知道了传输层两个协议的特点和应用场景后，就很容易判断某个应用层协议在传输层使用什么协议了。

现在判断一下，QQ聊天在传输层使用的是什么协议，QQ传文件在传输层使用的是什么协议？

如果使用QQ给好友传输文件，且传输文件会持续几分钟或几十分钟，则肯定不是使用一个数据包就能把文件传输完的。我们需要将要传输的文件分段传输，在传输文件之前需要建立会话，并在传输过程中实现可靠传输、流量控制、拥塞避免等。我们需要在传输层中使用TCP来实现这些功能。

使用QQ聊天时，通常一次输入的聊天内容不会有太多文字，使用一个数据包就能把聊天内容发送出去。并且聊完第一句，也不一定什么时候聊第二句，此时发送数据是不持续的。若发送QQ聊天的内容需在传输层使用UDP。

可见，应用程序通信可根据通信的特点来在传输层中选择不同的协议。

2.3.2 TCP首部

接下来讲解TCP报文的首部格式。TCP能够实现数据分段传输、可靠传输、流量控制、网络拥塞避免等功能。TCP报文首部比UDP报文首部的字段要多，并且首部长度不固定。如图2-27所示，TCP报文段首部

的前20字节是固定的，后面有4*N*个字节是根据需要而增加的选项（*N*是整数）。因此TCP首部的最小长度是20字节。

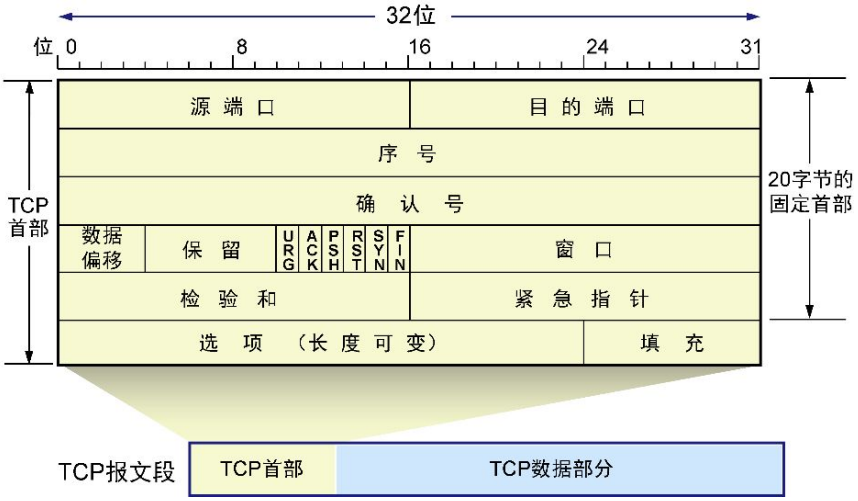


图2-27　TCP首部

首部固定部分各字段的意义如下。

（1）源端口和目的端口各占2字节，分别写入源端口号和目的端口号。

（2）序号占4字节。序号范围是[0, 2^{32}1]，共2^{32}（即4 294 967 296）个序号。序号增加到2^{32}1后，下一个序号就又回到0。TCP是面向字节流的。在一个TCP连接中传送的字节流中的每一个字节都按顺序编号。整个要传送的字节流的起始序号必须在连接建立时设置。首部中的序号字段值则指的是本报文段所发送的数据的第一个字节的序号。如图2-28所示，以A计算机给B计算机发送一个文件为例来说明序号的用法。为了方便说明问题，传输层其他字段没有展现，第1个报文段的序号字段值是1，而携带的数据共有100字节。这就表明：本报文段的

数据的第一个字节的序号是1，最后一个字节的序号是100。下一个报文段的数据序号应当从101开始，即下一个报文段的序号字段值应为101。这个字段的名称也叫作“报文段序号”。

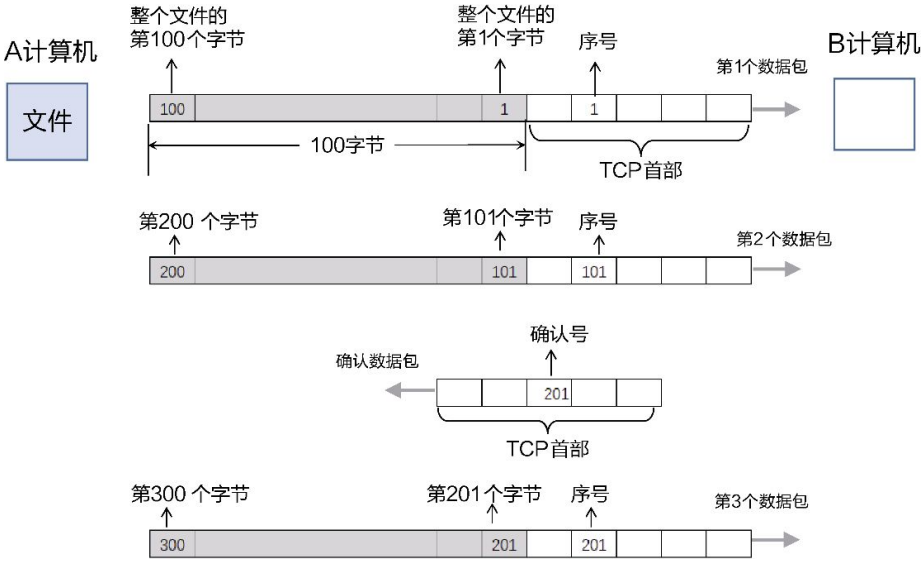


图2-28　理解序号和确认号

B计算机将收到的数据包放到缓存，根据序号对收到的数据包中的字节进行排序，B计算机的程序会从缓存中读取编号连续的字节。

（3）确认号。确认号占4字节，是期望收到对方下一个报文段的第一个数据字节的序号。

TCP能够实现可靠传输。接收方收到几个数据包后，就会给发送方一个确认数据包，告诉发送方下一个数据包该发第多少个字节了。如图2-28所示的例子，B计算机收到了两个数据包，将两个数据包字节排序得到连续的前200字节，B计算机要发一个确认包给A计算机，告诉A

计算机应该发送第201字节了，这个确认数据包的确认号就是201。确认数据包没有数据部分，只有TCP首部。

总之，应当记住：若确认号是*N*，则表明到序号*N*-1为止的所有数据都已正确收到。

序号字段有32位长，可对4GB（即4千兆字节）的数据进行编号。如果传输的文件大于4GB，则序号就会再次从1开始。

（4）数据偏移占4字节。它指出TCP报文段的数据起始处距离TCP报文段的起始处有多远。这个字段实际上指出了TCP报文段的首部长度。由于首部中还有长度不确定的选项字段，因此数据偏移字段是必要的。但请注意，“数据偏移”的单位为4字节，由于4位二进制数能够表示的最大十进制数是15，因此数据偏移的最大值是60字节，这也是TCP首部的最大长度，也就意味着选项长度不能超过40字节。

（5）保留占6字节。保留一般是后面会使用，目前应置为0。

（6）紧急URG（urgent）。当URG=1时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传送（相当于高优先级的数据），而不要按原来的排队顺序传送。例如，已经发送了一个很长的程序要在远地的主机上运行。但后来发现了一些问题，需要取消该程序的运行。因此用户从键盘发出中断命令（Control+C）。如果不使用紧急数据，那么这两个字符将存储在接收TCP的缓存末尾。只有在所有的数据被处理完毕后这两个字符才被交付到接收方的应用进程。这样做就浪费了许多时间。

当URG置1时，发送应用进程就告诉发送方的TCP有紧急数据要传送。于是发送方TCP就把紧急数据插入到本报文段数据的最前面，而在紧急数据后面的数据仍是普通数据。URG要与首部中的紧急指针（Urgent Pointer）字段配合使用。

（7）确认ACK（acknowlegment）。仅当ACK=1时确认号字段才有效。当ACK=0时，确认号字段无效。TCP规定，在连接建立后所有传送的报文段都必须把ACK置1。

（8）推送PSH（push）。当两个应用进程进行交互式的通信时，有时一端的应用进程希望在键入一个命令后立即就能收到对方的响应。在这种情况下，TCP就可以使用推送（push）操作。即发送方TCP把PSH置1，并立即创建一个报文段发送出去。接收方TCP收到PSH=1的报文段后，就尽快地（即“推送”向前）交付给接收应用进程，而不再等到整个缓存都填满了后再向上交付。虽然应用程序可以选择推送操作，但推送操作很少使用。

（9）复位RST（reset）。当RST=1时，表明TCP连接中出现严重差错（如主机崩溃或其他原因），必须释放连接，然后再重新建立传输连接。RST置1还用来拒绝一个非法的报文段或拒绝打开一个连接。RST也可称为重建位或重置位。

（10）同步SYN（synchronization），在连接建立时用来同步序号。当SYN=1而ACK=0时，表明这是一个连接请求报文段。对方若同意建立连接，则应在响应的报文段中使SYN=1和ACK=1。因此，SYN置为1

就表示这是一个连接请求或连接接受报文。关于连接的建立和释放，在后面TCP连接管理部分将详细讲解。

（11）终止FIN（finish），用来释放一个连接。当FIN=1时，表明此报文段的发送方的数据已发送完毕，并要求释放传输连接。

（12）窗口，占2字节。窗口值是[0,$2^{16}-1$]的整数。TCP有流量控制功能，窗口值用来告诉对方：从本报文段首部中的确认号算起，接收方目前允许对方发送的最大数据量（单位是字节）。之所以要有这个限制，是因为接收方的数据缓存空间是有限的。总之，窗口值作为接收方让发送方设置其发送窗口的依据。使用TCP传输数据的计算机会根据自己的接收能力随时调整窗口值，然后对方参照这个值及时调整发送窗口，从而达到流量控制功能。

（13）检验和占2字节。检验和字段检验的范围包括首部和数据两部分。

（14）紧急指针占2字节。紧急指针仅在URG=1时才有意义，它指出本报文段中的紧急数据的字节数（紧急数据结束后就是普通数据）。因此紧急指针指出了紧急数据的末尾在报文段中的位置。当所有紧急数据都处理完后，TCP就告诉应用程序恢复正常操作。值得注意的是，即使窗口为零时也可发送紧急数据。

（15）选项的长度可变，最长可达40字节。当没有使用选项时，TCP的首部长度是20字节。TCP最初只规定了一种选项，即最大报文段长度（Maximum Segment Size，MSS）。MSS是每一个TCP报文段中的数

据字段的最大长度。数据字段加上TCP首部才等于整个TCP报文段，因此MSS并不是整个TCP报文段的最大长度，而是“TCP报文段长度减去TCP首部长度”。

2.3.3 TCP连接管理

TCP是可靠传输协议，使用TCP通信的计算机在正式通信之前需要先确保对方是否存在，并协商通信的参数，比如接收端的接收窗口大小、支持的最大报文段长度（MSS）、是否允许选择确认（SACK）、是否支持时间戳等。建立连接后就可以进行双向通信了，通信结束后，释放连接。

TCP连接的建立采用客户/服务器方式。主动发起连接建立的应用进程叫作客户端（Client），而被动等待连接建立的应用进程叫作服务端（Server）。

1. TCP的连接建立

如图2-29所示，客户端向服务端发起通信，客户端的TCP模块与服务端的TCP模块之间将通过“3次握手”（Three-way Handshaking）来建立TCP会话。

所谓3次握手，是指在TCP会话的建立过程中总共交换了3个TCP控制段， 这3个数据包就是TCP建立连接的数据包。

TCP建立连接的过程如图 2-29 所示，不同阶段在客户端和服务器端能够看到不同的状态。

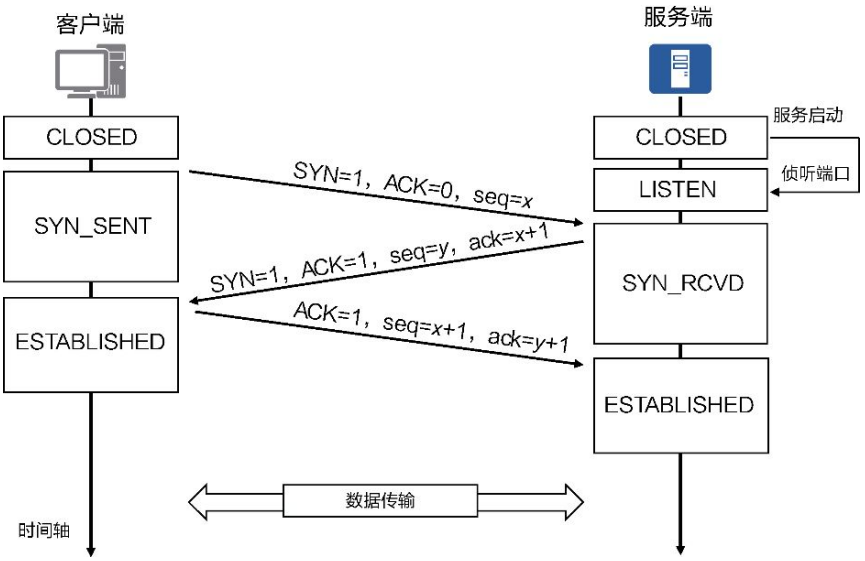


图2-29　用3次握手建立TCP连接

服务端启动服务后，就会使用TCP的某个端口侦听客户端的请求，等待客户的连接，状态由CLOSED变为LISTEN状态。

3次握手具体如下。

（1）客户端的应用程序发送TCP连接请求报文，把自己的状态告诉对方，这个报文的TCP首部SYN标记位是1，ACK标记位为0，序号（seq）为x，这个x被称为客户端的初始序列号，通常为0。发送出连接请求报文后，客户端就处于SYN_SENT状态。

（2）服务端收到客户端的TCP连接请求后，发送确认连接报文，将自己的状态告诉给客户端，这个报文的TCP首部SYN标记位是1，ACK

标记位为1，确认号（ack）为x+1，序号（seq）为y，y为服务端的初始序列号。服务器端此时处于SYN_RCVD状态。

（3）客户端收到连接请求确认报文后，状态就变为ESTABLISHED，然后再次发送给服务器一个确认报文，用于确认会话的建立。该报文SYN标记位为0，ACK标记位为1，确认号（ack）为y+1。服务器端收到确认报文后，状态变为ESTABLISHED。

需要特别注意的是，经过3次握手之后，A、B之间其实是建立起了两个TCP会话，一个是从客户端指向服务端的TCP会话，另一个是从服务端指向客户端的TCP会话。A是发起通信的一方，说明客户端有信息要传递给服务端，于是客户端首先发送了一个SYN段，请求建立一个从客户端指向服务端的TCP会话，这个会话的目的是要控制信息能够正确且可靠地从客户端传递给服务端。服务端在收到SYN段后，会发送一个SYN+ACK段作为回应。SYN+ACK段的含义是：服务端一方面同意了客户端的请求，另一方面也请求建立一个从服务端指向客户端的TCP会话，这个会话的目的是要控制信息能够正确且可靠地从服务端传递给客户端。客户端收到SYN+ACK段后，回应一个ACK段，表示同意服务端的请求。

以后就可以进行双向可靠通信了。

2．TCP连接释放

TCP通信结束后，需要释放连接。TCP连接释放过程比较复杂，我们结合双方状态的改变来阐明连接释放的过程。数据传输结束后，通信的双方都可释放连接。如图2-30所示，现在A和B都处于ESTABLISHED状态，A的应用进程先向其TCP发出连接释放报文段，并停止发送数据，主动关闭TCP连接。A把连接释放报文段首部的FIN置1，其序号seq=u，它等于前面已传送过的数据的最后一个字节的序号加1。这时A进入FIN-WAIT-1（终止等待1）状态，等待B的确认。

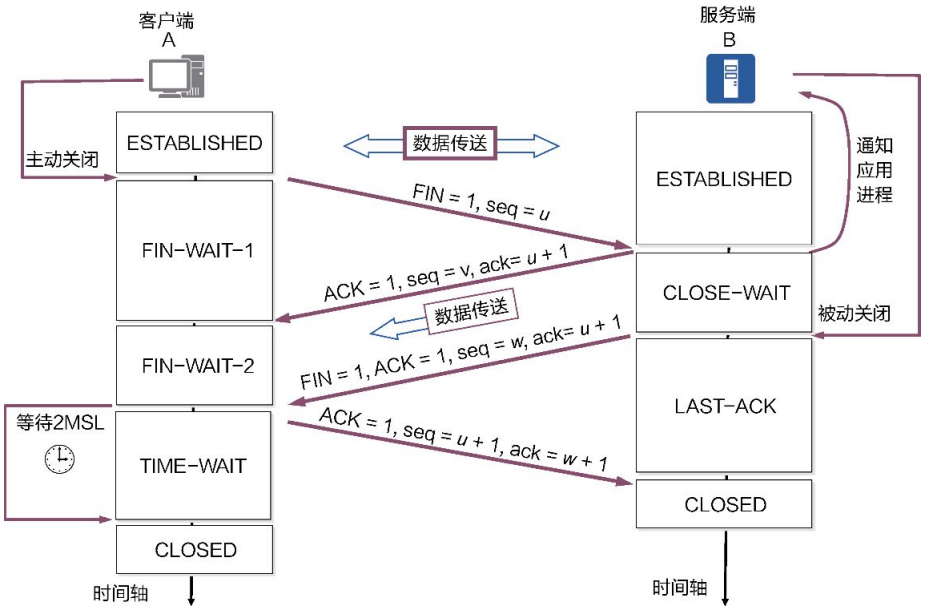


图2-30　TCP连接释放的过程

请注意，TCP规定，FIN报文段即使不携带数据，也会消耗掉一个序号。

B收到连接释放报文段后立即发出确认，确认号是ack=u+1，而这个报文段自己的序号是v，等于B前面已传送过的数据的最后一个字节的序号加1。然后B就进入CLOSE-WAIT（关闭等待）状态。TCP服务器进

程这时应通知高层应用进程，从而从A到B这个方向的连接就释放了，这时的TCP连接处于半关闭（half-dose）状态，即A已经没有数据要发送了，但若B发送数据，A仍要接收。也就是说，从B到A这个方向的连接并未关闭。这个状态可能会持续一些时间。

A收到来自B的确认后，就进入FIN-WAIT-2（终止等待2）状态，然后等待B发出连接释放报文段。若B已经没有要向A发送的数据，那么其应用进程就通知TCP释放连接。这时B发出的连接释放报文段必须使FIN=1。现假定B的序号为w（在半关闭状态B可能又发送了一些数据）。B还必须重复上次已发送过的确认号ack=u+1。这时B就进入LAST-ACK（最后确认）状态，等待A的确认。

A在收到B的连接释放报文段后，必须对此发出确认。在确认报文段中把ACK置1，确认ack=w+1，而自己的序号seq=u+1（根据TCP标准，前面发送过的FIN报文段要消耗一个序号）。然后进入到TIME-WAIT（时间等待）状态。请注意，现在TCP连接还没有释放掉。必须经过时间等待计时器（TIME-WAIT timer）设置的时间2MSL后，A才进入CLOSED状态。时间MSL叫作最长报文段寿命（Maximum Segment Lifetime），RFC793建议设为2分钟。但这完全是从工程上来考虑的，对于现在的网络，MSL=2分钟可能太长了。因此TCP允许不同的实现可根据具体情况使用更小的MSL值。因此，从A进入到TIME-WAIT状态后，要经过4分钟才能进入到CLOSED状态，才能开始建立下一个新的连接。

上述的TCP连接释放过程是4次握手，也可以看成是两个二次握手。除时间等待计时器外，TCP还设有一个保活计时器（Keepalive

Timer）。设想有这样的情况：客户已主动与服务器建立了TCP连接，但后来客户端的主机突然出现故障。显然，服务器以后就不能再收到客户发来的数据了。因此，应当有措施使服务器不会再白白等待下去。这就要使用保活计时器。服务器每收到一次客户的数据，就重新设置保活计时器，时间的设置通常是两小时。若两小时后没有收到客户的数据，服务器就发送一个探测报文段，以后则每隔75分钟发送一次。若一连发送10个探测报文段后仍无客户的响应，服务器就认为客户端出了故障，接着就关闭这个连接。

2.3.4 TCP可靠传输的实现

TCP实现可靠传输使用的是连续自动重传请求（Automatic Repeat-reQuest，ARQ）协议和滑动窗口协议。下面就介绍连续ARQ和滑动窗口协议的工作过程。

TCP建立连接后，双方可以使用建立的连接相互发送数据。为了更方便地讨论问题，我们仅考虑A发送数据而B接收数据并发送确认。因此A叫作发送方，B叫作接收方。

滑动窗口是面向字节流的，为了方便大家记住每个分组的序号，下面的讲解就假设每一个分组是100字节。为了方便画图，我将分组进行编号以简化表示，如图2-31所示。不过你要记住，每一个分组的序号是多少。

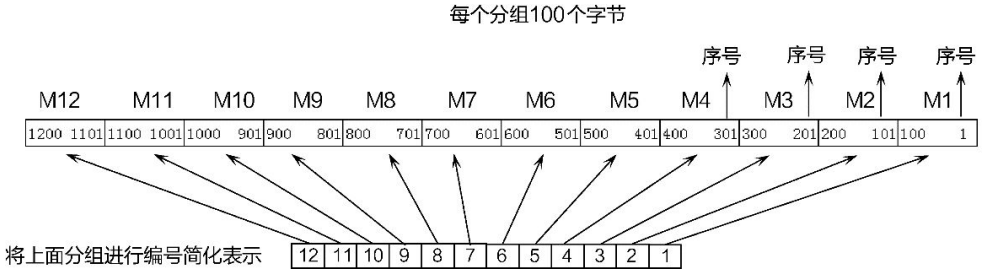


图2-31　简化分组表示

如图2-32所示，在建立TCP连接时，B计算机告诉A计算机它的接收窗口为400字节，A计算机就设置一个400字节大小的发送窗口。如果一个分组有100字节，那么在发送窗口中就有M1、M2、M3和M4 4个分组，发送端A就可以连续发送这4个分组，每一个分组都记录一个发送时间，如图2-32中 $t1$时刻所示，发送完毕后，就停止发送。接收端B收到这4个连续分组，只需给A发送一个确认，确认号为401，告诉A计算机401以前的字节已经全部收到。在 $t2$时刻，发送端A收到M4分组的确认，发送窗口就向前滑动，M5、M6、M7和M8分组就进入发送窗口，这4个分组就可以连续发送。发送完后，停止发送，等待确认。这就是滑动窗口协议。

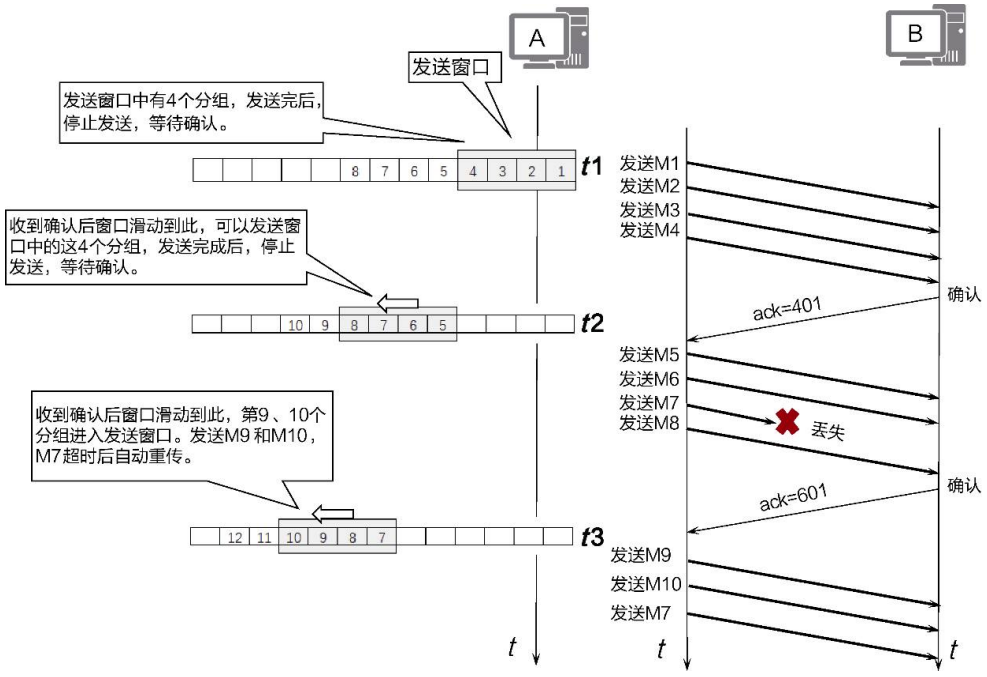


图2-32　连续ARQ协议和滑动窗口协议

如果M7在传输过程中丢失，B计算机只收到M5、M6和M8分组。B收到连续的M1、M2……M6分组，就会给A计算机发送一个确认，该确认的序号为601，告诉A计算机600以前的字节全部收到。在$t3$时刻，A计算机收到确认，但并不是立即发送M7，而是向前滑动发送窗口，M9和M10进入发送窗口，发送M9和M10。什么时候发送M7呢？M7超时后就会自动重发。这个超时时间是一个比往返时间长一点的时间。如果发送了M9之后M7就超时了，此时发送顺序就变成了M9、M7和M10。这就是连续ARQ协议。

2.3.5　UDP

UDP与TCP一样用于处理数据包。在OSI模型中，两者都位于传输层，处于IP的上一层。传输层中的UDP是一个无连接的传输协议，UDP

为应用程序提供了一种无须建立连接就可以发送封装的 IP 数据包的方法。

UDP的缺点为不提供数据包分组和组装的功能，且不能对数据包进行排序，也就是说，当报文发送之后，我们是无法得知其是否安全、完整到达的。UDP用来支持那些需要在计算机之间传输数据的网络应用。包括网络视频会议系统在内的众多的客户/服务器模式的网络应用都需要使用UDP。UDP从问世至今已经被使用了很多年，虽然其最初的光彩已经被一些类似协议所掩盖，但即使在今天UDP仍然不失为一项非常实用和可行的网络传输层协议。

许多应用只支持UDP，如多媒体数据流，它不产生任何额外的数据，即使知道有破坏的包也不进行重发。当强调传输性能而不是传输的完整性时，如音频和多媒体应用，UDP是最好的选择。

2.3.6 传输层协议和应用层协议之间的关系

TCP/IP中的应用层协议很多，而传输层只有两个协议，如何使用两个传输层协议来标识应用层协议呢？

传输层协议加一个端口号可以标识一个应用层协议。如图2-33所示，图中标明了传输层协议和应用层协议之间的关系。

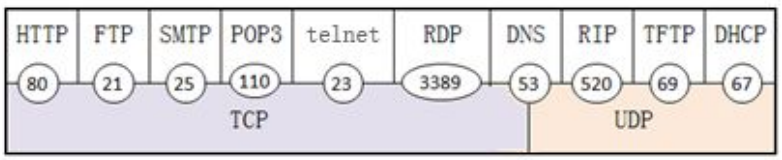


图2-33　传输层协议和应用层协议之间的关系

DNS同时占用UDP和TCP端口53是公认的，通过抓包分析，几乎所有的情况在使用UDP，这说明DNS主要还是使用UDP。DNS在进行区传送的情况下会使用TCP（区传送是指一个区域内主DNS服务器和辅助DNS服务器之间建立通信连接并进行数据传输的过程），这个存在疑问？

下面是一些常见的应用层协议和传输层协议之间的关系。

- HTTP默认使用TCP的80端口。
- FTP默认使用TCP的21端口。
- SMTP默认使用TCP的25端口。
- POP3默认使用TCP的110端口。
- HTTPS默认使用TCP的443端口。
- DNS使用TCP/UDP的53端口。
- telnet使用TCP的23端口。
- RDP远程桌面协议默认使用TCP的3389端口。

以上列出的都是默认端口，当然也可以更改应用层协议使用的端口。如果不使用默认端口，客户端访问服务器时需要指明所使用的端口。比如91学IT网站指定HTTP使用808端口，访问该网站时就需要指明使用的端口：http://www.91xueit.com:808，冒号后面的808指明HTTP使用端口808。如图2-34所示，远程桌面协议（RDP）没有使用默认端口，冒号后面的9090指定使用端口9090。

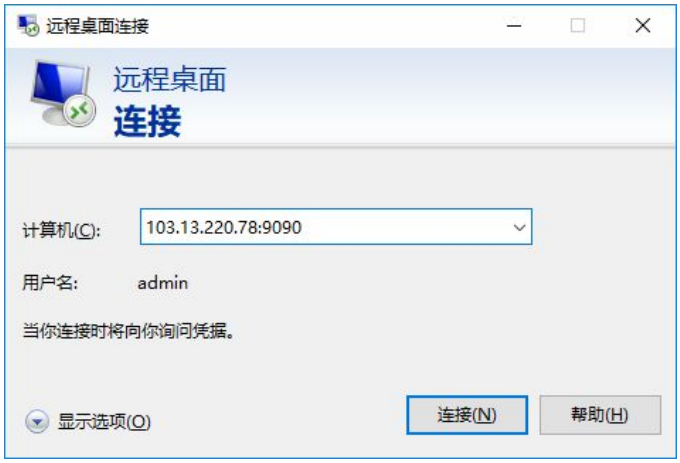


图2-34　为远程桌面协议指定使用的端口

如图 2-35 所示，一台服务器同时运行了Web服务、SMTP服务和POP3服务，Web服务一启动就用TCP的80端口侦听客户端请求，SMTP服务一启动就用TCP的25端口侦听客户端请求，POP3服务一启动就用TCP的110端口侦听客户端请求。现在网络中的A计算机、B计算机和C计算机分别打算访问端口服务器的Web服务、SMTP服务和POP3服务。它们发送3个数据包①、②、③，这3个数据包的目标端口分别是80、25和110，服务器收到这3个数据包后，就根据目标端口将数据包提交给不同的服务进行处理。



图2-35　应用层协议和传输层协议之间的关系

现在大家就会明白，数据包的目标IP地址用来定位网络中的某台服务器，目标端口用来定位服务器上的某个服务。

图2-35给大家展示了A、B、C计算机访问服务器的数据包，该数据包目标端口和源端口，源端口是计算机临时为客户端程序分配的，服务器向A、B、C计算机发送数据包时，源端口就会变成目标端口。

如图 2-36 所示，A计算机打开谷歌浏览器，一个窗口访问百度网站，另一个窗口访问51CTO网页，这就需要建立两个TCP连接。A计算机会给每个窗口临时分配一个客户端端口（要求本地唯一），从51CTO返回的数据包的目标端口是13456，从百度网站返回的数据包的目标端口是12928，这样A计算机就知道这些数据包来自哪个网站，应给哪一个窗口。

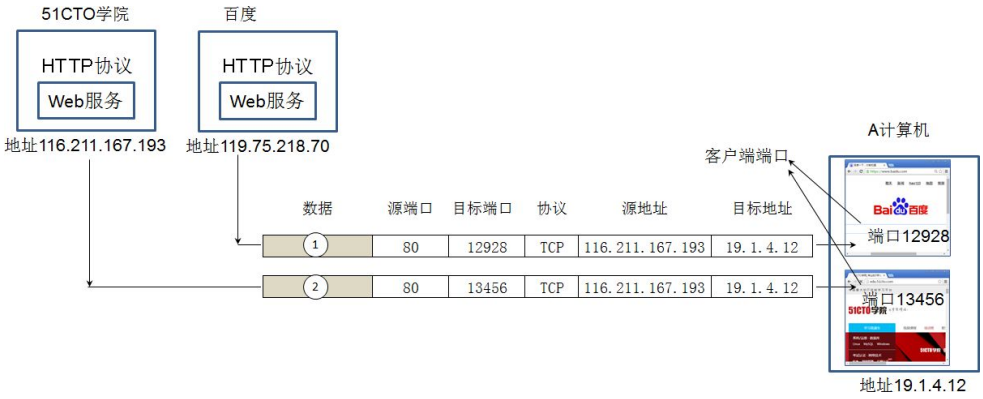


图2-36　源端口的作用

传输层使用16位二进制来标识一个端口，端口号的取值范围是0～65535，这个数目对一台计算机来说足够用了。

端口号分为如下两大类。

（1）服务器端使用的端口号。

服务器端使用的端口号在这里又分为两类，最重要的一类叫作熟知端口号（well-known port number）或系统端口号，取值范围为0～1023。这些数值可从iana网站中查到。iana把这些端口号指派给了TCP/IP中非常重要的一些应用程序，并让所有的用户都知道。下面给出一些常用的熟知端口号，如图2-37所示。

应用程序或服务	FTP	telnet	SMTP	DNS	TFTP	HTTP	SNMP
熟知端口号	21	23	25	53	69	80	161

图2-37　熟知端口号

另一类叫作登记端口号，取值范围为1024～49151。这类端口号由没有熟知端口号的应用程序使用。要使用这类端口号，必须在iana中按照规定的手续登记，以防止重复。

（2）客户端使用的端口号。

当打开浏览器访问网站，或登录QQ等客户端软件和服务器建立连接时，计算机会为客户端软件分配临时端口，这就是客户端端口，取值范围为49152～65535。由于这类端口号仅在客户进程运行时才动态选择，因此又叫作临时（短暂）端口号。这类端口号留给客户进程暂时使用。当服务器进程收到客户进程的报文时，就知道了客户进程所使用的端口号，因而可以把数据发送给客户进程。通信结束后，刚才已使用过的客户端口号就不复存在。这个端口号就可以供其他客户进程以后使用。

2.3.7　服务和端口之间的关系

计算机之间的通信，通常是服务器端程序（以后简称服务）运行等待客户端程序的连接请求。服务端器程序通常以服务的形式存在于Windows服务系统或Linux系统中。这些服务不需要用户登录服务器，系统启动后就可以自动运行。

服务运行后就要使用TCP或UDP的某个端口侦听客户端的请求，服务停止，则端口关闭，同一台计算机的不同服务使用的端口不能冲突（端口唯一）。

在Windows Server 2003系统中，在命令提示符下输入netstat -an可以查看侦听的端口，如图2-38所示。

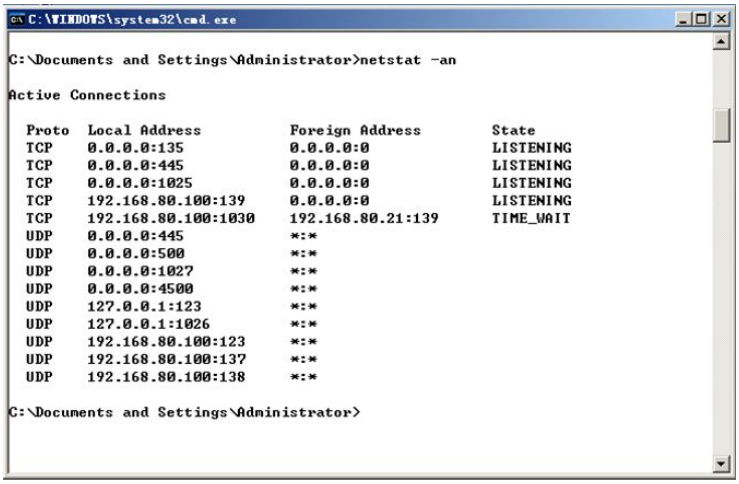


图2-38　Windows系统侦听的端口

如图2-39所示，设置Windows Server 2003系统属性。启用远程桌面（相当于启用远程桌面服务）后，再次运行netstat-an就会看到侦

听的端口多了TCP的3389端口。关闭远程桌面，再次查看侦听端口，可以看到不再侦听3389端口。

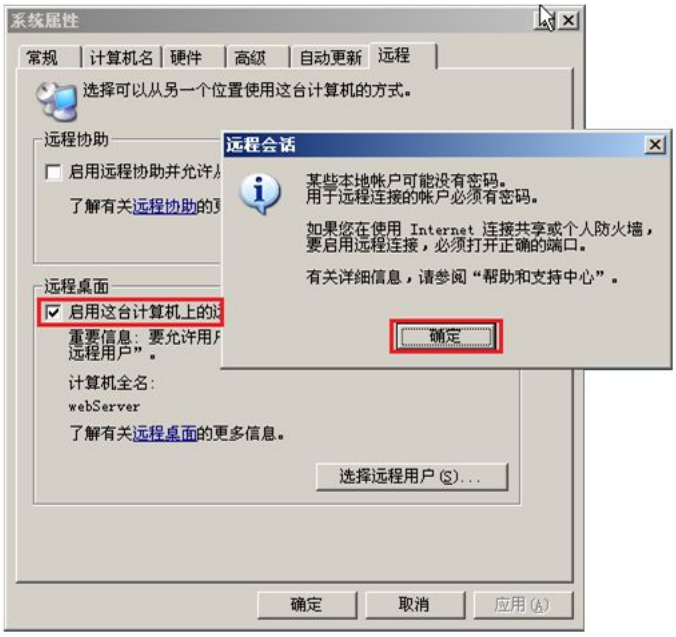


图2-39　设置Windows Server 2003启用远程桌面

如图2-40所示，在命令提示符下使用telnet命令可以测试远程计算机是否侦听了某个端口，只要telnet没有提示端口打开失败，就意味着远程计算机侦听该端口。使用端口扫描工具也可以扫描远程计算机打开的端口，如果服务使用默认端口，那么根据服务器侦听的端口就能判断远程计算机开启了什么服务。你就明白了那些黑客入侵服务器时，为啥需要先进行端口扫描，扫描端口就是为了明白服务器开启了什么服务，知道运行了什么服务才可以进一步检测该服务是否有漏洞，然后进行攻击。

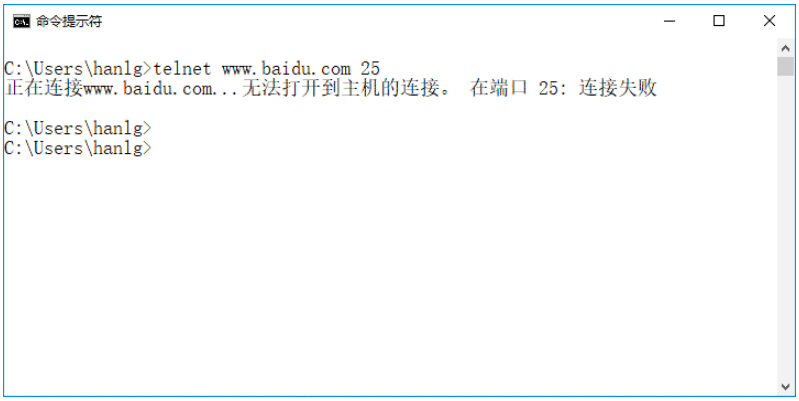


图2-40　测试百度网站是否侦听25端口

2.3.8　端口和网络安全的关系

客户端和服务器之间的通信使用应用层协议，应用层协议使用传输层协议+端口标识，知道了这个关系后，网络安全也就应该了解了。

如果在一台服务器上安装了多个服务，其中一个服务有漏洞，被黑客入侵，黑客就能获得操作系统的控制权，进一步破坏其他服务。

如图 2-41 所示，服务器对外提供 Web 服务，在服务器上还安装了微软的数据库服务（MySQL服务），网站的数据就存储在本地的数据库中。如果没有配置服务器的防火墙对进入的流量做任何限制，且数据库的内置管理员账户sa的密码为空或弱密码，那么网络中的黑客就可以通过TCP的1433端口连接到数据库服务，猜测数据库的sa账户的密码，一旦猜对，就能获得服务器上操作系统管理员的身份，对服务器进行任何操作，这就意味着服务器被入侵了。

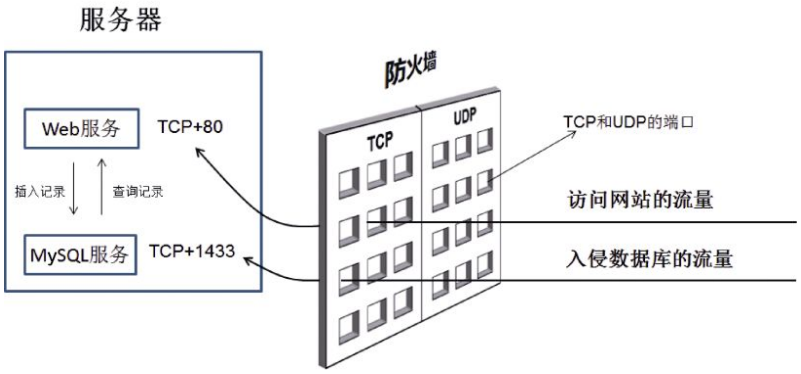


图2-41　服务器防火墙开放全部端口

TCP/IP在传输层中有两个协议：TCP和UDP，TCP和UDP就相当于网络中的两扇大门。如图2-41所示，门上开的洞就相当于开放TCP和UDP的端口。

如果想让服务器更加安全，那就把TCP和UDP这两扇大门关闭，在大门上只开放必要的端口。如图2-42所示，如果服务器对外只提供Web服务，便可以设置Web服务器防火墙只对外开放TCP的80端口，其他端口都关闭。这样即便服务器上运行了数据库服务，并使用TCP的1433端口侦听客户端的请求，互联网上的入侵者也没有办法通过数据库入侵服务器。

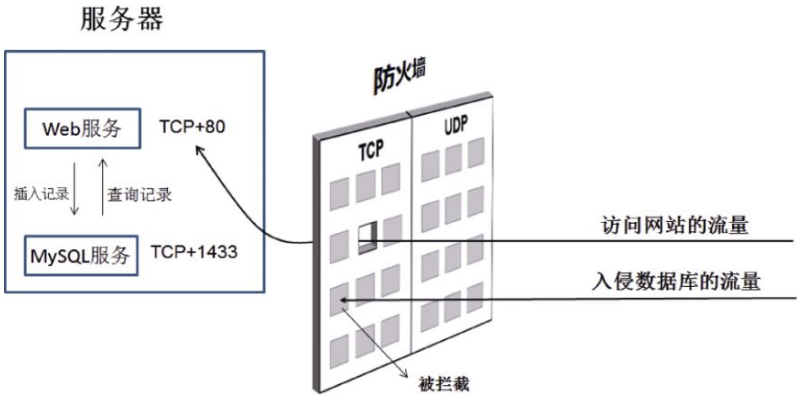


图2-42　在防火墙中设置对外开放的服务端口

前面讲的是设置服务器的防火墙，只开放必要的端口以加强服务器的网络安全。

我们也可以在路由器上设置网络防火墙，控制内网访问Internet的流量。如图2-43所示，企业路由器只开放了UDP的53端口和TCP的80端口，允许内网的计算机将域名解析的数据包发送到Internet的DNS服务器，并允许内网计算机使用HTTP访问Internet的Web服务器。内网计算机不能访问Internet上的其他服务，比如邮件发送（使用SMTP）和邮件接收（使用POP3协议）服务。

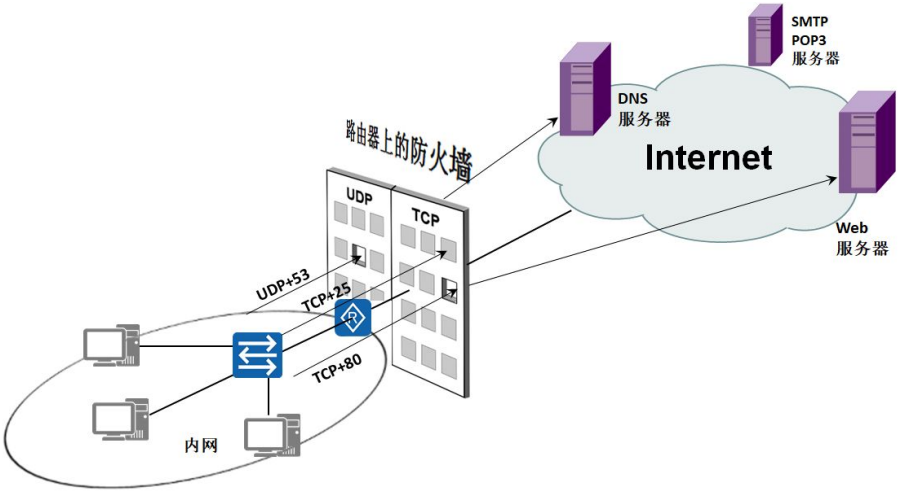


图2-43　在路由器上封锁端口

现在大家就会明白，如果我们不能访问某台服务器上的服务，也有可能是沿途路由器封掉了该服务使用的端口。在图2-43中，访问内网计算机telnet SMTP服务器的25端口就会失败，这并不是因为

Internet上的SMTP服务器上没有运行SMTP服务，而是沿途路由器封掉了访问SMTP服务器的端口。

2.4　网络层协议

2.4.1　网络层协议的两个版本

计算机通信使用的协议栈有两个，分别是TCP/IPv4协议栈和TCP/IPv6协议栈，TCP/IPv6相对于TCP/IPv4的网络层进行了改进，但两者实现的功能是一样的。

网络层协议为传输层提供服务，负责把传输层的段发送到接收端。IP实现网络层协议的功能，发送端将传输层的段加上IP首部。IP首部包括源IP地址和目标IP地址，加了IP首部的段称为“数据包”，网络中的路由器根据IP首部转发数据包。

如图2-44所示，TCP/IPv4协议栈的网络层有4个协议：ARP、IP、ICMP和IGMP。TCP和UDP使用端口号标识应用层协议，TCP段、UDP报文、ICMP报文、IGMP报文都可以封装在IP数据包中，使用协议号区分，也就是说IP使用协议号标识上层协议，TCP的协议号是6，UDP的协议号是17，ICMP的协议号是1，IGMP的协议号是2。虽然ICMP和IGMP都在网络层，但从关系上来看ICMP和IGMP在IP之上，也就是ICMP和IGMP的报文要封装在IP数据包中。

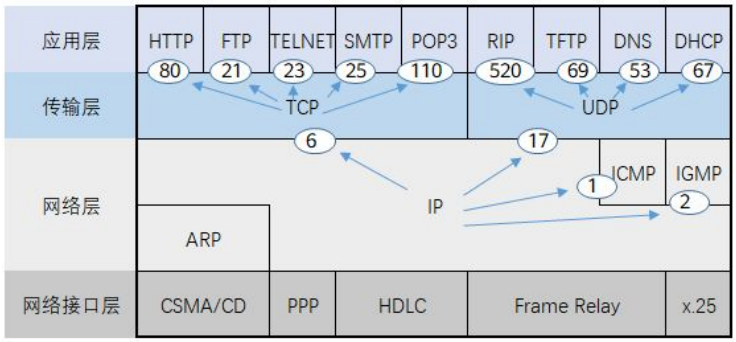


图2-44　TCP/IPv4协议栈

ARP在以太网中使用，用来将通信的目标地址解析为MAC地址，跨网段通信，并解析网关的MAC地址。解析出MAC地址才能将数据包封装成帧发送出去，因此ARP为IP提供服务，虽然将其归属到网络层，但从关系上来看ARP位于IP之下。

图2-45所示的是TCP/IPv6协议栈，它的网络层协议有了较大变化，但网络层功能和IPv4一样。

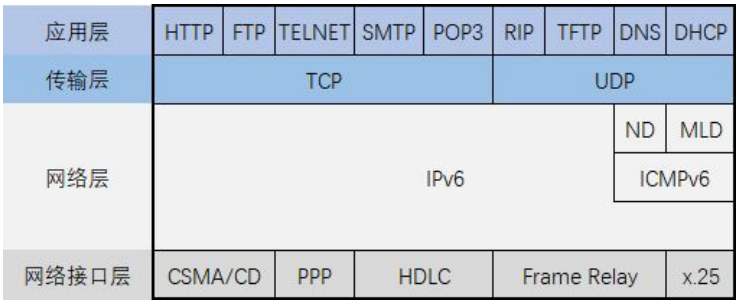


图2-45　TCP/IPv6协议栈

可以看到，IPv6协议栈与IPv4协议栈相比，只是网络层发生了变化，不会影响TCP和UDP，也不会影响数据链路层协议，网络层的功能和IPv4一样。IPv6的网络层没有ARP和IGMP，对ICMP的功能做了很大的扩展。IPv4协议栈中ARP的功能和IGMP的多点传送控制功能也被嵌入到

ICMPv6中，分别是邻居发现（Neighbor Discovery，ND）协议和多播侦听器发现（Multicast Listener Discovery，MLD）协议。

IPv6在本书后面章节详细讲解，在这里不做过多讲述。

2.4.2 IPv4

不做特别说明，IP默认是指IPv4。IP（Internet Protocol）又称网际协议，它负责Internet上网络之间的通信，并规定了将数据从一个网络传输到另一个网络应遵循的规则。它是TCP/IP的核心。

IP 是点到点的。它很简单，但不能保证传输的可靠性。它采用的是无连接数据报机制，对数据是“尽力传递”，不验证正确与否，也不保证分组顺序，且不发确认。所以IP提供的是主机间不可靠的无连接数据报传送。

IP的任务是对数据报进行相应的寻址和路由选择，并将其从一个网络转发到另一个网络。IP在每个要发送的数据包前加入控制信息（IP首部），其中包含了源主机的IP地址、目的主机的IP地址和其他一些信息。如果目的主机直接连在本网络中，那么IP可直接通过网络将数据报发给目的主机。如果目的主机在远端网络中，IP则通过路由器传送数据报，而路由器则依次通过下一网络将数据报传送到目的主机或再下一个路由器，即一个IP数据报通过互联网络，从一个IP模块传到另一个IP模块，直到终点为止。

IP数据包首部的格式能够说明IP都具有什么功能。在TCP/IP的标准中，各种数据格式常常以32位（即4字节）为单位来描述。图2-46是IP数据包的完整格式。



图2-46　网络层首部格式

IP数据包由首部和数据两部分组成。首部的前一部分是固定部分，共20字节，是所有IP数据包必须有的。在首部的固定部分的后面是可变部分，它是一些可选字段，其长度是可变的。

下面就网络层首部固定部分的各个字段进行详细讲解。

（1）版本占4位，指IP的版本。IP目前有两个版本IPv4和IPv6。通信双方使用的IP版本必须一致。目前广泛使用的IP版本号为4（即IPv4）。

（2）首部长度占4位，可表示的最大十进制数值是15。请注意，这个字段所表示的数的单位是32位二进制数（即4字节），因此，当IP的首部长度为1111时（即十进制的15），首部长度就达到60字节。当IP分组的首部长度不是4字节的整数倍时，必须利用最后的填充字段加以填充。因此数据部分永远以4字节的整数倍开始，这样在实现IP时较

为方便。首部长度限制为60 字节的缺点是有时可能不够用。但这样做是希望用户尽量减少开销。最常用的首部长度是20字节（即首部长度为0101），这时不使用任何选项。

正是因为首部长度有可变部分，所以才需要有一个字段来指明首部长度，如果首部长度是固定的也就没有必要有“首部长度”这个字段了。

（3）区分服务占8位。配置计算机给特定应用程序的数据包添加一个标志，然后再配置网络中的路由器优先转发这些带标志的数据包，在网络带宽比较紧张的情况下，也能确保这种应用的带宽有保障，这就是区分服务。这个字段在旧标准中叫作服务类型，但实际上一直没有被使用过。1998年IETF把这个字段改名为区分服务（Differentiated Service，DS）。只有在使用区分服务时，这个字段才起作用。

（4）总长度指IP首部和数据的长度，也就是数据包的长度，单位为字节。总长度字段为16位，因此数据包的最大长度为$2^{16}1$=65535字节。实际上传输这样长的数据包在现实中是极少遇到的。

（5）标识（identification）占16位。IP在存储器中维持着一个计数器，每产生一个数据包，计数器就加1，并将此值赋给标识字段。但这个“标识”并不是序号，因为IP是无连接服务，所以数据包不存在按序接收的问题。当数据包由于长度超过网络的MTU而必须分片时，同一个数据包被分成多个片，这些片的标识都一样，也就是数据包中

标识字段的值被复制到所有的数据包分片的标识字段中。相同的标识字段的值使分片后的各数据包片能正确地重装成为原来的数据包。

（6）标志（flag）占3位，但目前只有两位有意义。

标志字段中的最低位记为MF（more fragment）。MF=1表示后面还有“分片”的数据包。MF=0表示这是若干数据包片中的最后一个。

标志字段中间的一位记为DF（don’t fragment），意思是“不能分片”。只有当DF=0时才允许分片。

（7）片偏移占13位。片偏移指出：较长的分组在分片后，某片在原分组中的相对位置。也就是说，相对于用户数据字段的起点，片偏移指出该片从何处开始。片偏移以8字节为偏移单位。这就是说，每个分片的长度一定是8字节（64位）的整数倍。

（8）生存时间。生存时间字段常用的英文缩写是TTL（Time To Live），表示数据包在网络中的寿命。由发出数据包的源点设置这个字段，其目的是防止无法交付的数据包无限制地在网络中兜圈子（例如从路由器R1，转发到R2，再转发到R3，然后又转发到R1，从而白白消耗网络资源）。最初的设计是以秒作为TTL值的单位。每经过一个路由器时，就在TTL中减去数据包在路由器所消耗的时间。若数据包在路由器消耗的时间小于1秒，就把TTL值减1。当TTL值减为零时，就丢弃这个数据包。

然而随着技术的进步，路由器处理数据包所需的时间不断在缩短，一般都远远小于1秒，后来就把TTL字段的功能改为“跳数限制”（但名称不变）。路由器在转发数据包之前就把TTL值减1。若TTL值减小到零，就丢弃这个数据包，不再转发。因此，现在TTL的单位不再是秒，而是跳数。TTL的意义是指明数据包在网络中至多可经过多少个路由器。显然，数据包能在网络中经过的路由器的最大数值是255。若把TTL的初始值设置为1，就表示这个数据包只能在本局域网中传送。这个数据包一传送到局域网上的某个路由器，在被转发之前TTL值就减小到零，从而就会被这个路由器丢弃。

（9）协议占 8 位，协议字段指出此数据包携带的数据使用何种协议，以便使目的主机的网络层知道应将数据部分上交给哪个处理过程。常用的一些协议和相应的协议字段值如图 2-47所示。

协议名	ICMP	IGMP	IP	TCP	EGP	IGP	UDP	IPv6	ESP	OSPF
协议字段值	1	2	4	6	8	9	17	41	50	89

图2-47　协议号

（10）首部检验和占16位，这个字段只检验数据报的首部，但不检验数据部分。这是因为数据报每经过一个路由器，路由器都要重新计算一下首部检验和（一些字段，如生存时间、标志、片偏移等可能发生变化）。不检验数据部分可减少计算的工作量。

（11）源IP地址占32位。

（12）目标IP地址占32位。

2.4.3 ICMP

ICMP Internet控制报文协议（Internet Control Message Protocol，ICMP）是TCP/IPv4协议栈中网络层的一个协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。

ICMP报文是在IP数据报内部被传输的，它封装在IP数据报内。ICMP报文通常被IP层或更高层的协议（TCP或UDP）使用。一些ICMP报文把差错报文返回给用户进程。

接下来以抓包查看ICMP报文的格式。如图2-48所示，用PC1 ping PC2，ping命令产生一个ICMP请求报文，该报文被发送给目标地址，用来测试网络是否畅通。如果目标计算机收到ICMP请求报文，就会返回ICMP响应报文。下面的操作就是使用抓包工具捕获链路上ICMP请求报文和ICMP响应报文，请观察这两种报文的区别。

如图2-48所示，捕获AR1和AR2路由器链路上的数据包。

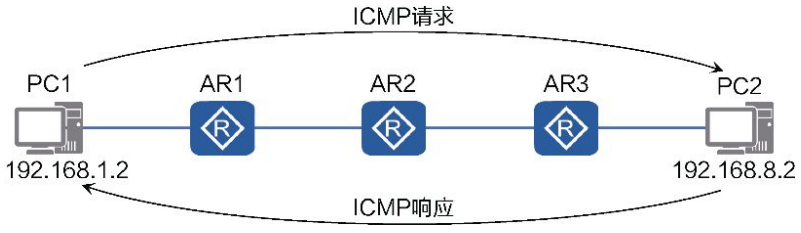


图2-48　ICMP请求和响应报文

图2-49所示的是ICMP请求报文，请求报文中有ICMP报文类型字段、ICMP报文代码字段、校验和字段以及ICMP数据部分。请求报文类型的值为8，报文代码为0。

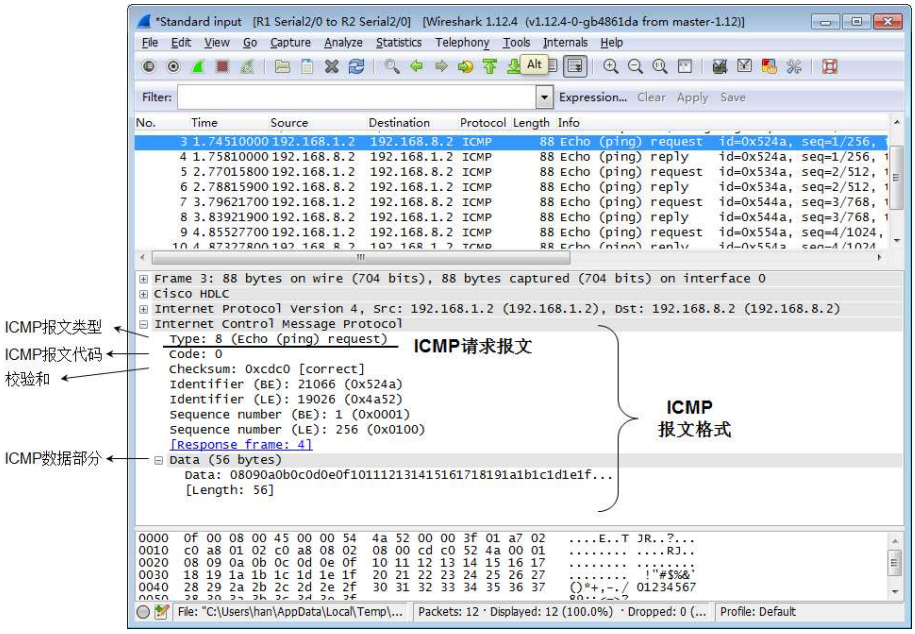


图2-49　ICMP请求报文

图2-50所示的是ICMP响应报文，响应报文类型的值为0，报文代码为0。

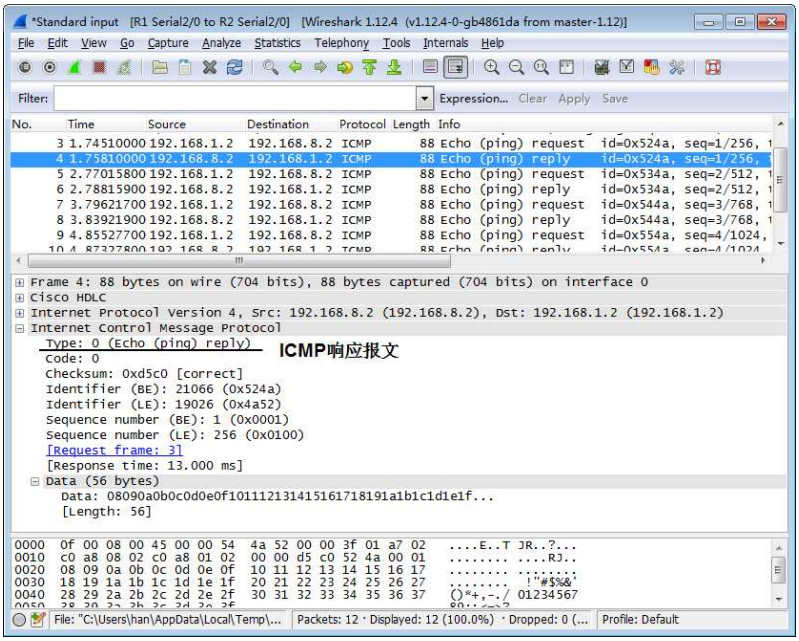


图2-50　ICMP响应报文

ICMP报文分几种类型，每种类型又使用代码来进一步指明ICMP报文所代表的不同的含义。表2-1列出了常见的ICMP报文的类型和代码，以及代码所代表的含义。

表2-1 ICMP报文类型和代码代表的意义

报 文 种 类	类 型 值	代 码	描 述
请求报文	8	0	请求回显报文
响应报文	0	0	回显应答报文
差错报告报文	3（终点不可到达）	0	网络不可达
		1	主机不可达
		2	协议不可达
		3	端口不可达
		4	需要进行分片，但设置了不分片
		13	由于路由器过滤，通信被禁止
	4	0	源端被关闭
	5（改变路由）	0	对网络重定向

		1	对主机重定向
	11	0	传输期间生存时间（TTL）为0
	12（参数问题）	0	坏的IP首部
		1	缺少必要的选项

ICMP差错报告共有5种，具体如下。

（1）终点不可到达。当路由器或主机没有到达目标地址的路由时，就丢弃该数据包，给源点发送终点不可到达报文。

（2）源点抑制。当路由器或主机由于拥塞而丢弃数据包时，就会向源点发送源点抑制报文，使源点知道应当降低数据包的发送速率。

（3）时间超时。当路由器收到生存时间为零的数据报时，除丢弃该数据报外，还要向源点发送时间超过报文。当终点在预先规定的时间内不能收到一个数据报的全部数据报片时，就把已收到的数据报片都丢弃，并向源点发送时间超过报文。

（4）参数问题。当路由器或目的主机收到的数据报的首部中有的字段的值不正确时，就丢弃该数据报，并向源点发送参数问题报文。

（5）改变路由（重定向）。路由器把改变路由报文发送给主机，让主机知道下次应将数据报发送给另外的路由器（可通过更好的路由）。

ping命令并不能跟踪数据包从源地址到目标地址沿途经过了哪些路由器，而在Windows操作系统中，华为路由器可以使用tracert命令跟踪数据包转发路径，能够帮助我们发现在到达目标地址的众多链路

中到底是哪一条链路出现了故障。tracert命令是ping命令的扩展，它用IP报文生存时间（TTL）字段和ICMP差错报告报文来确定沿途经过的路由器。

不使用tracert命令，使用ping命令也可以得到到达目标地址沿途经过的路由器。如图2-51所示，如何在PC1上测试到达PC2所途经的路由器呢？下面演示如何使用ping命令和-i参数确定数据包到达目的地途经的路由器。

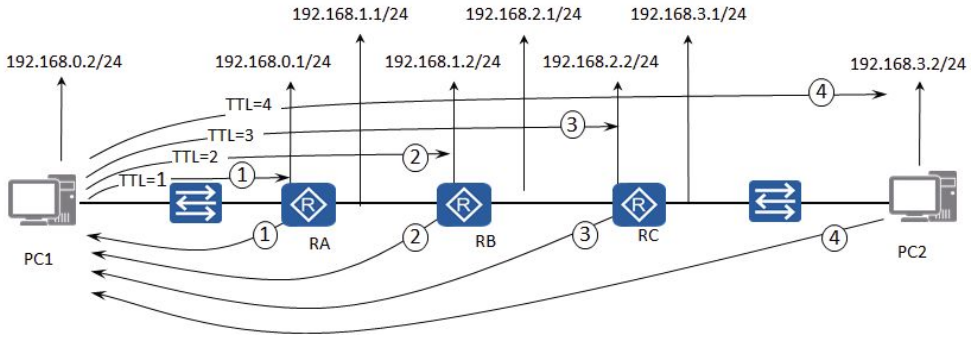


图2-51　使用ping和-i参数跟踪数据包路径

（1）在PC1上ping PC2的地址：ping 192.168.3.2 -i 1，给目标地址发送ICMP请求数据包时指定TTL=1，就会由第1个路由器RA返回一个TTL耗尽的ICMP差错报告报文，PC1得到途经的第1个路由器的地址192.168.0.1。

```
C:\Users\han>ping 192.168.3.2 -i 1
正在 Ping 192.168.3.2 具有 32 字节的数据:
来自 192.168.0.1 的回复: TTL 传输中过期。
来自 192.168.0.1 的回复: TTL 传输中过期。
来自 192.168.0.1 的回复: TTL 传输中过期。
来自 192.168.0.1 的回复: TTL 传输中过期。
```

（2）PC1再次ping PC2的地址：ping 192.168.3.2 -i 2，给目标地址发送ICMP请求数据包时指定TTL=2，就会由第2个路由器RB返回一个TTL耗尽的ICMP差错报告报文，PC1得到途经的第2个路由器的地址192.168.1.2。

（3）以此类推，PC1再次ping PC2的地址，指定TTL为3，就能得到第3个路由器RC的地址192.168.2.2。

tracert命令的工作原理就是使用上述方法，给目标地址发送TTL逐渐增加的ICMP请求，根据返回的ICMP错误报告报文来确定沿途经过的路由器。

PC1通过路由器返回的TTL耗尽的ICMP报文得到沿途的全部路由器。如果出现有的路由器不允许发送TTL差错报告报文的情况，那么使用tracert将不能得知该路由器。

如图2-52所示，tracert 91XUEIT网站途经17个路由器，第18个是该网站的地址（终点）。可以看到第12、第16和第17个路由器显示“请求超时”，这表明没有返回ICMP差错报告报文，因为这些路由器设置了访问控制列表（ACL）禁止路由器发出ICMP差错报告报文。

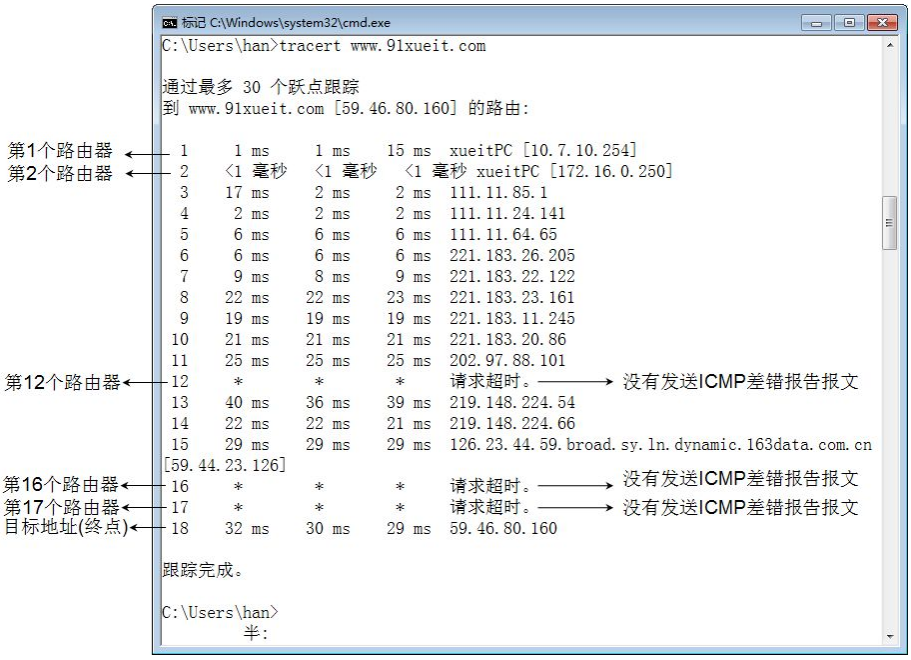


图2-52　跟踪数据包路径

tracert能够帮助我们发现路由配置错误的问题。观察图2-53中tracert的结果，能得到什么结论？你会发现数据包在172.16.0.2和172.16.0.1两个路由器之间往复转发，可以断定问题就出在这两个路由器的路由配置上，需要检查这两个路由器的路由表。



图2-53　数据包在两个路由器之间往复转发

2.4.4 ARP

网络层协议还包括ARP，该协议只在以太网中使用，用来将计算机的IP地址解析出MAC地址。

如图2-54所示，网络中有两个以太网和一个点到点链路。计算机和路由器接口的地址在图2-54中标出，图中的MA、MB、……、MH代表对应接口的MAC地址。下面介绍计算机A和本网段计算机C的通信过程，以及计算机A和计算机H的跨网段通信过程。

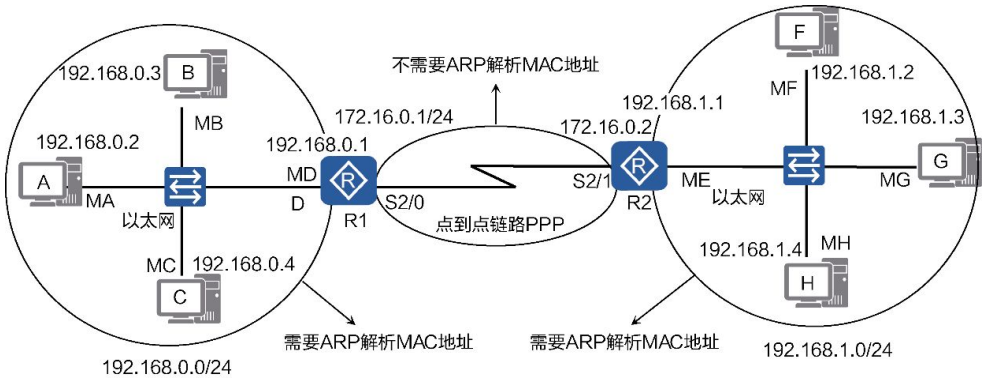


图2-54　以太网需要ARP

如果计算机A ping计算机C的地址192.168.0.4，计算机A判断出目标IP地址和自己在一个网段，那么数据链路层封装的目标MAC地址就是计算机C的MAC地址，图2-55所示的是计算机A发送给计算机C的帧。

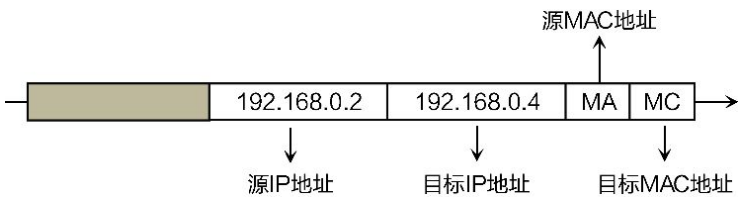


图2-55　同一网段的帧

如果计算机A ping计算机H的地址192.168.1.4，计算机A判断出目标IP地址和自己不在一个网段，那么数据链路层封装的目标MAC地址是网关的MAC地址，也就是路由器R1的D接口的MAC地址，如图2-56所示。



图2-56　跨网段的帧

计算机接入以太网后，只给计算机配置了IP地址、子网掩码和网关，并没有告诉它网络中其他计算机的MAC地址。计算机和目标计算机通信前必须知道目标MAC地址，问题来了，计算机A是如何知道计算机C的MAC地址或网关的MAC地址的？

TCP/IP协议栈的网络层有ARP（Address Resolution Protocol）。在计算机和目标计算机通信之前，需要使用该协议解析到目标计算机的MAC地址（同一网段通信）或网关的MAC地址（跨网段通信）。

这里大家需要知道：ARP只是在以太网中使用，点到点链路使用PPP通信，PPP帧根本不需要地址，所以也不用ARP解析MAC地址。

图2-57所示的是使用抓包工具捕获的ARP请求数据包，第27帧是计算机192.168.80.20解析192.168.80.30的MAC地址发送的ARP请求数据包。注意观察目标MAC地址为ff: ff: ff: ff: ff: ff。其中Opcode是

选项代码，指示当前包是请求报文还是应答报文，ARP请求报文的值是0×0001，ARP应答报文的值是0×0002。

ARP是建立在网络中各个主机互相信任的基础上的，计算机A发送ARP广播帧解析计算机C的MAC地址，同一个网段中的计算机都能够收到这个ARP请求消息，任何一个主机都可以给计算机A发送ARP应答消息。主机可能会告诉计算机A一个错误的MAC地址，计算机A收到ARP应答报文时并不会检测该报文的真实性，直接将其记入本机ARP缓存，这样就存在一个安全隐患——ARP欺骗。

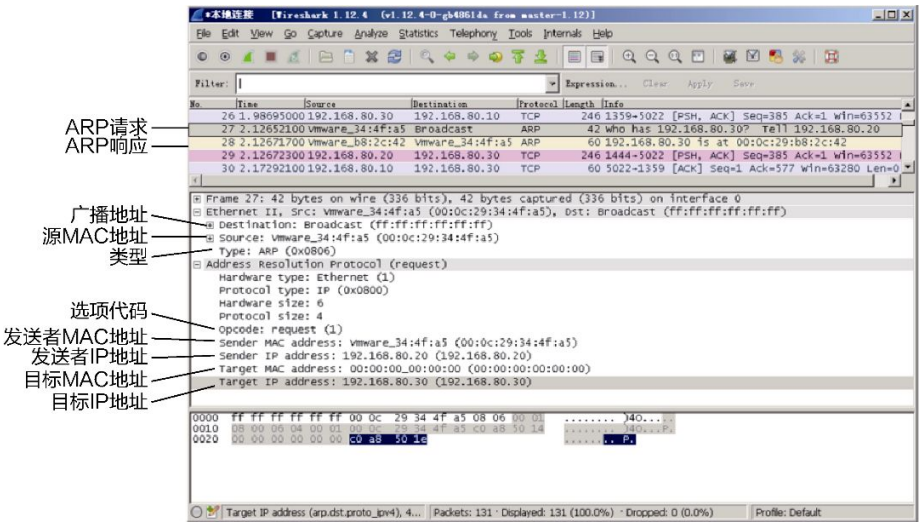


图2-57　ARP请求帧

在Windows系统中运行arp -a可以查看缓存的IP地址和MAC地址的对应表。

```
C:\Users\hanlg>arp -a
接口: 192.168.2.161 --- 0xb
  Internet 地址          物理地址              类型
  192.168.2.1           d8-c8-e9-96-a4-61     动态
  192.168.2.169         04-d2-3a-67-3d-92     动态
```

```
  192.168.2.182         c8-60-00-2e-6e-1b       动态
  192.168.2.219         6c-b7-49-5e-87-48       动态
  192.168.2.255         ff-ff-ff-ff-ff-ff       静态
```

2.4.5 IGMP

Internet组管理协议（Internet Group Management Protocol，IGMP），是因特网协议家族中的一个组播协议。该协议运行在主机和组播路由器之间。

IGMP提供了在转发组播数据包到目的地的最后阶段所需的信息，实现如下双向的功能：

- 主机通过IGMP通知路由器希望接收或离开某个特定组播组的信息；
- 路由器通过IGMP周期性地查询局域网内的组播组成员是否处于活动状态，实现所连网段组成员关系的收集与维护。

IGMP共有3个版本，即IGMP v1、IGMP v2和IGMP v3。

本书对IGMP不做过多介绍，读者若有需求可参考其他资料。

2.5　数据链路层协议

数据链路层协议负责将帧从链路的一端传到另一端。如图2-58所示，PC1给PC2通信，需要经过链路1、链路2、……、链路6。数据链路层协议负责将网络层的数据包封装成帧，将帧从链路的一端发送到另一端。

在图2-58中，计算机连接交换机的链路是以太网链路，使用的是带冲突检测的载波监听多路访问技术（Carrier Sense Multiple Access with Collision Detection，CSMA/CD）协议，该协议定义的帧成为以太网帧，以太网帧包含源MAC地址和目标MAC地址这些字段。路由器和路由器之间的连接为点到点连接，针对这种链路的数据链路层协议有点对点协议（Point-to- Point，PPP）、高级数据链路控制（High-Level Data Link Control，HDLC）等。不同的数据链路层协议定义了不同的帧格式。

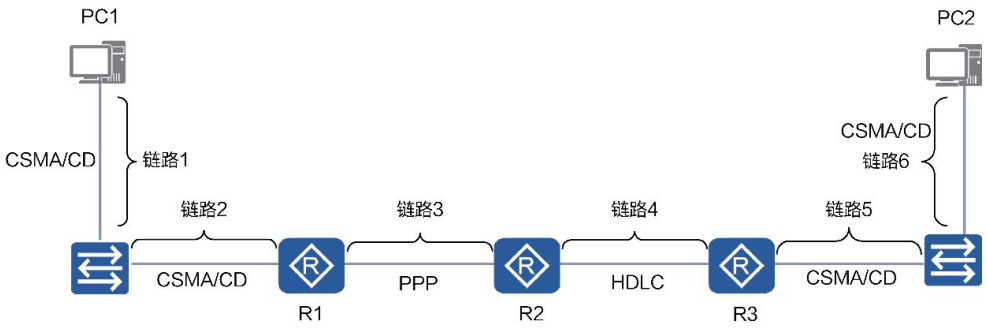


图2-58　链路和数据链路层协议

数据链路层的协议有许多种，但有3个基本问题是共同的。这3个基本问题是：封装成帧、透明传输和差错检测。下面针对这3个问题进

行详细讨论。

（1）封装成帧。

封装成帧，就是在网络层的IP数据报的前后分别添加首部和尾部，这样就构成了一个帧。不同的数据链路层协议的帧的首部和尾部包含的信息有明确的规定，如图2-59所示，帧的首部和尾部有帧开始符和帧结束符，称为帧定界符。接收端收到物理层传过来的数字信号并读取到帧开始符，然后一直读到帧结束符，就认为接收到了一个完整的帧。

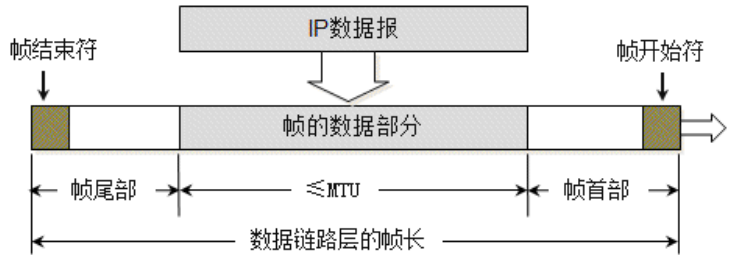


图2-59　帧首部和帧尾部封装成帧

若数据传输过程出现差错，那么帧定界符的作用更加明显。如果发送端在尚未发送完一个帧时突然出现故障，中断发送，接收端收到了只有帧开始符没有帧结束符的帧，就认为是一个不完整的帧，必须丢弃。

为了提高数据链路层的传输效率，应当使帧的数据部分尽可能地大于首部和尾部的长度。但是每一种数据链路层协议都规定了所能够传送帧的数据部分长度的上限，即最大传输单元（Maximum Transfer

Unit，MTU），以太网的MTU为1500字节，如图2-59所示，MTU指的是数据部分长度。

（2）透明传输。

帧开始符和帧结束符最好选择不会出现在帧的数据部分的字符，如果帧数据部分出现帧的开始符和帧结束符，就要插入转义字符，接收端看到转义字符就去掉，然后把转义字符后面的字符当作数据来处理。这就是透明传输。

如图2-60所示，某数据链路层协议的帧开始符为SOH，帧结束符为EOT。转义字符选定为ESC。节点A给节点B发送数据帧，在被发送到数据链路之前，数据中出现SOH、ESC和EOT字符，现在需要在编码之前的位置插入转义字符ESC，这个过程就是字节填充。节点B接收到数据之后，再去掉填充的转义字符，视转义字符后的字符为数据。

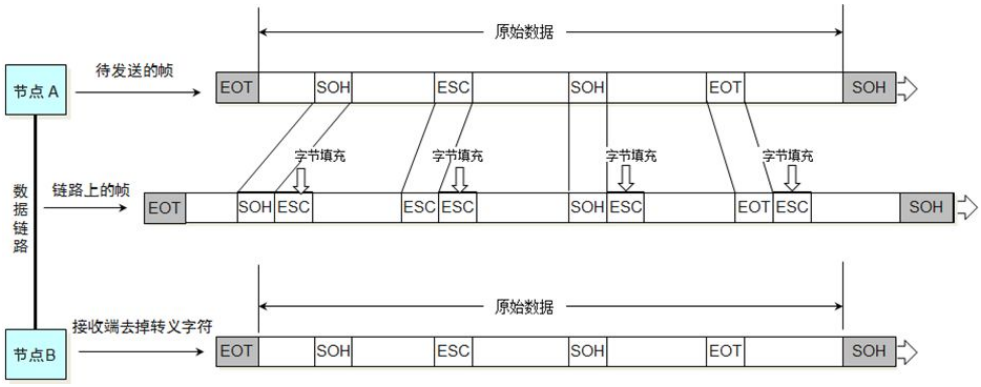


图2-60　使用字节填充法解决透明传输的问题

发送节点A在发送帧之前要在原始数据中的必要位置处插入转义字符，接收节点B收到后去掉转义字符，重新得到原始数据，插入转义字

符是要让传输的原始数据原封不动地到达节点B，这个过程称为“透明传输”。

（3）差错检验。

现实的通信链路不会都是理想的。这就是说，比特在传输过程中可能会产生差错：1可能会变成0，而0也可能变成1，这就叫作比特差错。比特差错是传输差错中的一种。在一段时间内，传输错误的比特占所传输比特总数的比率称为误码率（Bit Error Rate，BER）。例如，误码率为10^{10}，表示平均每传送10^{10}比特就会出现一个比特的差错。误码率与信噪比有很大的关系。提高信噪比就可以使误码率降低。但实际的通信链路并非理想的，它不可能使误码率下降到零。因此，为了保证数据传输的可靠性，在计算机网络传输数据时，必须采用各种差错检验措施。目前在数据链路层广泛使用的是循环冗余检验（Cyclic Redundancy Check，CRC）的差错检验技术。

要想让接收端能够判断帧在传输过程是否出现差错，则需要在传输的帧中包含用于检测错误的信息，这部分信息就叫作帧校验序列（Frame Check Sequence，FCS）。如图2-61所示，使用帧的数据部分和数据链路层首部来计算FCS，然后将其放到帧的末尾。接收端收到数据后，再使用数据部分和数据链路层首部计算一个FCS，比较两个FCS是否相同，如果相同则认为在传输过程中没有出现差错。如果出现差错，接收端丢弃该帧。

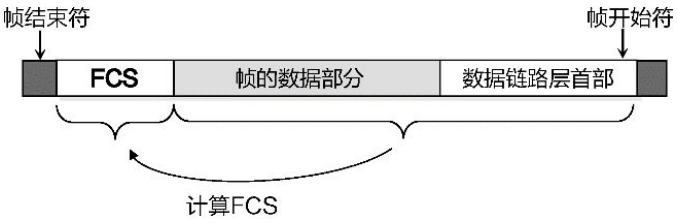


图2-61　帧校验序列

2.6　物理层协议

物理层协议定义了与传输媒体的接口有关的一些特性，如接口标准，有了接口标准，各厂家生产的网络设备接口才能相互连接和通信。比如定义了以太网接口标准，不同厂家的以太网设备就能相互连接。物理层为数据链路层提供服务。

物理层包括以下几方面的定义，也可以认为是物理层协议包括的内容。

（1）机械特性，指明接口所用接线器的形状和尺寸、引脚数目和排列、固定的锁定装置等，常见的各种规格的接插部件都有严格的标准化规定。这很像常见的各种规格的电源插头，其尺寸都有严格的规定。图2-62所示的是某广域网接口和线缆接口。



图2-62　某广域网接口和线缆接口

（2）电气特性，指明在接口电缆的各条线上出现的电压范围，比如−10V～10V。

（3）功能特性，指明某条信号线上出现的某一电平的电压表示何种意义。

（4）过程特性，定义在信号线上进行二进制比特流传输的一组操作过程，包括各信号线的工作顺序和时序，使得比特流传输得以完成。

2.7 OSI参考模型和TCP/IP

前面给大家讲的TCP/IPv4协议是互联网通信的工业标准。当网络刚开始出现时，典型情况下只能在同一制造商制造的计算机产品之间进行通信。20世纪70年代后期，国际标准化组织（International Organization for Standardization，ISO）创建了开放系统互连（Open Systems Interconnection，OSI）参考模型，从而打破了这一壁垒。

OSI参考模型将计算机通信过程按功能划分为7层，并规定了每一层实现的功能。这样互联网设备的厂家以及软件公司就能参照OSI参考模型来设计自己的硬件和软件，不同供应商的网络设备之间就能够互相协同工作。

OSI参考模型不是具体的协议，TCP/IPv4协议栈是具体的协议，怎么来理解它们之间的关系呢？比如，国际标准组织定义了汽车参考模型，规定汽车要有动力系统、转向系统、制动系统、变速系统等，这就相当于OSI参考模型定义的计算机通信每一层要实现的功能。参照这个汽车参考模型汽车厂商可以研发自己的汽车，比如奥迪轿车，它实现了汽车参考模型的全部功能，此时奥迪汽车就相当于TCP/IP。奥迪轿车，动力系统有的使用汽油，有的使用天然气，发动机有的是8缸，有的是10缸，实现的功能都是汽车参考模型要求的动力系统功能。变速系统有的是手动挡，有的是自动挡，有的是4级变速，有的是6级变

速，有的是无级变速，实现的功能都是汽车参考模型要求的变速功能。

同样，OSI参考模型只定义了计算机通信每层要实现的功能，并没有规定如何实现以及实现的细节，不同的协议栈实现方法可以不同。

国际标准化组织（ISO）制定的OSI参考模型把计算机通信分成了7层。

（1）应用层。应用层协议实现应用程序的功能，将实现方法标准化就形成了应用层协议。互联网中的应用很多，比如访问网站、收发电子邮件、访问文件服务器等，因此应用层协议也很多。定义客户端能够向服务器发送哪些请求（命令），服务器能够向客户端返回哪些响应，以及用到的报文格式、命令的交互顺序，都是应用层协议应该包含的内容。

（2）表示层。应用程序要将传输的信息转换成数据。如果传输的是字符文件，那么要使用字符集将文件转换成数据。如果是图片或应用程序这些二进制文件，也要被编码变成数据，数据在传输前是否压缩、是否加密处理都是表示层要解决的问题。发送端的表示层和接收端的表示层是协议的双方，数据的加密和解密、压缩和解压缩、编码和解码等都要遵循表示层协议的规范。

（3）会话层。会话层为通信的客户端和服务端程序建立会话、保持会话和断开会话。建立会话：A、B两台计算机之间需要通信，要建立一条会话供它们使用，在建立会话的过程中会有身份验证、权限鉴

定等环节。保持会话：通信会话建立后，A、B两台计算机开始传递数据，当数据传递完成后，OSI会话层不一定立即将这条通信会话断开，它会根据应用程序和应用层的设置对会话进行维护，在会话维持期间，双方可以随时使用会话传输数据。断开会话：当应用程序或应用层规定的超时时间到期后，或A、B重启、关机或手动断开会话时，OSI会断开A、B之间的会话。

（4）传输层。传输层负责向两台主机进程之间的通信提供通用的数据传输服务。传输层有两种协议：传输控制协议（TCP）提供面向连接的、可靠的数据传输服务，其数据传输的单位是报文段；用户数据包协议（UDP）提供无连接的、尽最大努力的数据传输服务，其数据传输的单位是用户数据报。

（5）网络层。网络层为数据包跨网段通信选择转发路径。

（6）数据链路层。两台主机之间的数据通信，总是在一段一段的链路上传送的，这就需要专门的链路层协议。数据链路层就是将数据包封装成能够在不同链路上传输的帧。数据包在传递过程中要经过不同网络，比如集线器或交换机组建的网络就是以太网，以太网使用载波侦听多路访问协议（CSMA/CD），路由器和路由器之间的连接是点到点的链路，点到点链路可以使用PPP或帧中继（Frame Relay）协议。数据包要想在不同类型的链路传输就需要封装成不同的帧格式。比如以太网的帧，要加上目标MAC地址和源MAC地址，而点到点链路上的帧就不用添加MAC地址。

（7）物理层。物理层规定了网络设备的接口标准、电压标准，要是不定义这些标准，各个厂家生产的网络设备就不能连接到一起，更不可能相互兼容了。物理层也包括通信技术，那些专门研究通信的人就要想办法让物理线路（铜线或光纤）通过频分复用技术、时分复用技术或编码技术更快地传输数据。

TCP/IP分层对OSI参考模型进行了合并简化，其应用层实现了OSI参考模型的应用层、表示层和会话层的功能，TCP/IP分层还将数据链路层和物理层合并成网络接口层，如图2-63所示。

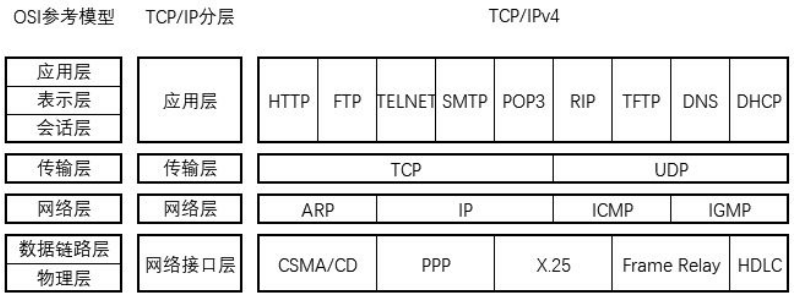


图2-63　OSI参考模型和TCP/IP分层

以下是将计算机通信分层的好处。

（1）各层之间是独立的。某一层并不需要知道它的下一层如何实现，仅需要知道该层通过层间接口所提供的服务。上层对下层来说就是要处理的数据，如图2-64所示。

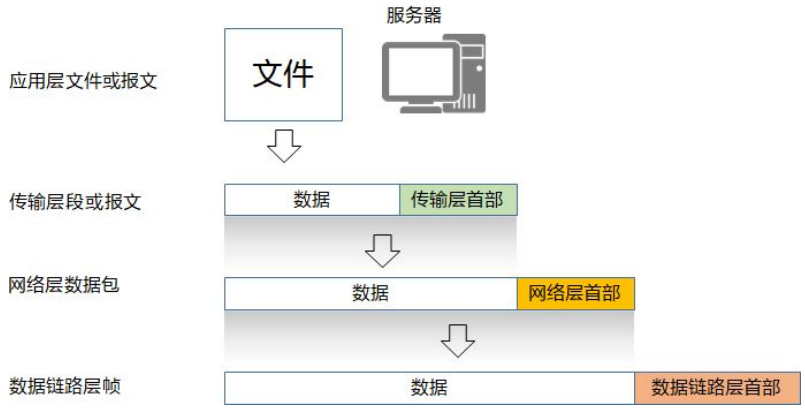


图2-64　各层之间的关系

（2）灵活性好。每一层的改进和变化不会影响其他层。比如IPv4实现的是网络层功能，升级为IPv6后，实现的仍然是网络层功能，传输层TCP和UDP不用做任何变动，数据链路层使用的协议也不用做任何变动。如图2-65所示，计算机可以使用IPv4和IPv6进行通信。

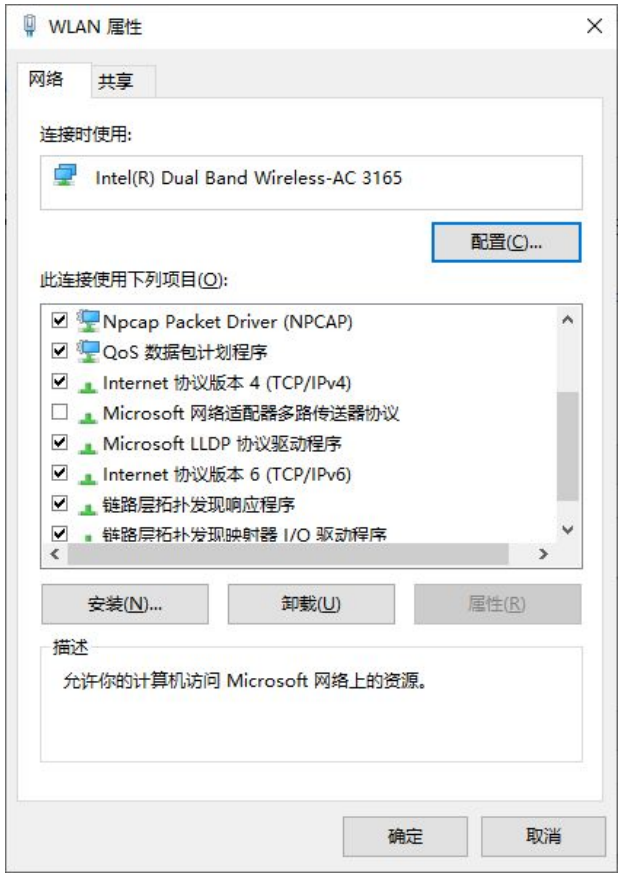


图2-65　IPv4和IPv6实现的功能一样

（3）各层都可以采用最合适的技术来实现，比如适合布线的就使用双绞线连接网络，有障碍物的就使用无线覆盖。

（4）促进标准化工作。路由器实现网络层功能，交换机实现数据链路层功能，不同厂家的路由器和交换机能够相互连接实现计算机通信，这是因为有了网络层标准和数据链路层标准。

（5）分层后有助于将复杂的计算机通信问题拆分成多个简单的问题，有助于排除网络故障。比如计算机没有设置网关造成的网络故障

属于网络层问题，MAC地址冲突造成的网络故障属于数据链路层问题，IE浏览器设置了错误的代理服务器访问不了网站，属于应用层问题。

2.8 习题

1．计算机通信实现可靠传输的是TCP/IP的哪一层？（　　）

A．物理层

B．应用层

C．传输层

D．网络层

2．由IPv4升级到IPv6，对TCP/IP来说是哪一层做了更改？（　　）

A．数据链路层

B．网络层

C．应用层

D．物理层

3．ARP有何作用？（　　）

A．将计算机的MAC地址解析成IP地址

B．域名解析

C．可靠传输

D．将IP地址解析成MAC地址

4．以太网使用什么协议在链路上发送帧？（　　）

A．HTTP

B．TCP

C．CSMA/CD

D．ARP

5．TCP和UDP端口号的范围是（　　）。

A．0～256

B．0～1023

C．0～65535

D．1024～65535

6．下列网络协议中，默认使用TCP端口号25的是（　　）。

A．HTTP

B．telnet

C. SMTP

D. POP3

7. 在Windows系统中，查看侦听的端口使用的命令是（　　）。

A. ipconfig /all

B. netstat -an

C. ping

D. telnet

8. 在Windows中，ping命令使用的协议是（　　）。

A. HTTP

B. IGMP

C. TCP

D. ICMP

9. 关于OSI参考模型中网络层的功能说法正确的是（　　）。

A. OSI参考模型中最靠近用户的一层，为应用程序提供网络服务

B. 在设备之间传输比特流，规定了电平、速度和电缆针脚

C．提供面向连接或非面向连接的数据传递以及进行重传前的差错检测

D．提供逻辑地址，供路由器确定路径

10．OSI参考模型从高层到低层分别是（　　）。

A．应用层、会话层、表示层、传输层、网络层、数据链路层、物理层

B．应用层、传输层、网络层、数据链路层、物理层

C．应用层、表示层、会话层、传输层、网络层、数据链路层、物理层

D．应用层、表示层、会话层、网络层、传输层、数据链路层、物理层

11．网络管理员能使用ping来测试网络的连通性，在这个过程中下面哪些协议可能会被使用到（　　）。（多选）

A．ARP

B．TCP

C．ICMP

D．UDP

12．计算机A给计算机D发送数据包要经过两个以太网帧，如图2-66所示，写出数据包的源IP地址和目标IP地址、源MAC地址和目标MAC地址。

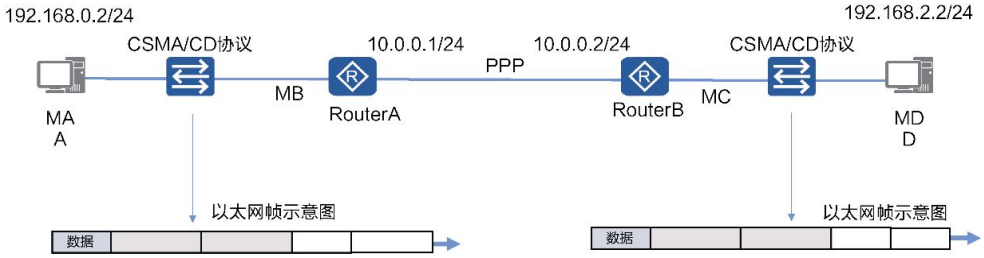


图2-66　计算机A与计算机D的通信示意图

13．TCP/IP按什么分层？写出每一层协议实现的功能。

14．列出几个常见的应用层协议。

15．应用层协议要定义哪些内容？

16．写出传输层的两个协议以及应用场景。

17．写出网络层的4个协议以及每个协议的功能。

第3章　IP地址和子网划分

本章内容

- IP地址层次结构
- IP地址分类
- 公网地址
- 私网地址
- 保留的IP地址
- 等长子网划分
- 变长子网划分
- 合并网段

本章讲解IP地址的格式、子网掩码的作用、IP地址的分类以及一些特殊的地址，介绍什么是公网地址和私网地址，以及私网地址如何通过NAT访问Internet。

为了避免IP地址的浪费，需要根据每个网段的计算机数量来分配合理的IP地址块，有可能需要将一个大的网段分成多个子网。本章讲解如何进行等长子网划分和变长子网划分。当然，如果一个网络中的计算机数量非常多，那么有可能一个网段的地址块容纳不下，也可以将多个网段合并成一个大的网段，这个大的网段就是超网。最后本章会介绍子网划分和合并网络的规律。

3.1　学习IP地址预备知识

网络中，计算机和网络设备接口的IP地址由32位的二进制数组成，在后面学习IP地址和子网划分时，需要我们将二进制数转化成十进制数，还需要将十进制数转化成二进制数。因此在学习IP地址和子网划分之前，先给大家补充一下二进制的相关知识，同时要求大家熟记下面讲到的二进制和十进制之间的关系。

3.1.1　二进制和十进制

学习子网划分需要读者看到一个十进制形式的子网掩码能很快判断出该子网掩码写成二进制形式有几个1；看到一个二进制形式的子网掩码，也能熟练写出该子网掩码对应的十进制数。

二进制是计算机技术中广泛采用的一种数制。二进制数据是用0和1两个数码来表示的数。它的基数为2，进位规则是“逢二进一”，借位规则是“借一当二”，当前的计算机系统使用的基本上是二进制。

下面所列的是二进制和十进制的对应关系。要求最好记住这些对应关系，其实也不用死记硬背，这里有规律可循，如下所示，二进制中的1向前移1位，对应的十进制乘以2。

二进制	十进制
1	1

10　　2

100　　4

1000　　8

1 0000　　16

10 0000　　32

100 0000　　64

1000 0000　　128

下面列出的二进制数和十进制数的对应关系最好也记住，要求做到：给出下面的一个十进制数，立即就能写出对应的二进制数；给出一个二进制数，能立即写出对应的十进制数。后面给出了记忆规律。

二进制　　十进制

1000 0000　　128

1100 0000　　192　　这样记 1000 0000+100 0000也就是128+64=192

1110 0000　　224　　这样记1000 0000+100 0000+10 0000也就是128+64+32=224

1111 0000　　240　　这样记128+64+32+16=240

1111 1000　　248　　这样记128+64+32+16+8=248

1111 1100　　252　　这样记128+64+32+16+8+4=252

1111 1110　　254　　这样记128+64+32+16+8+4+2=254

1111 1111　　255　　这样记128+64+32+16+8+4+2+1=255

可见8位二进制数的最大值就是255。

万一忘记了上面的对应关系，可以使用下面的方法。如图3-1所示，只要记住数轴上的几个关键点，对应关系立刻就能想出来。我们画一条线，左端代表二进制数0000 0000，右端代表二进制数1111 1111。

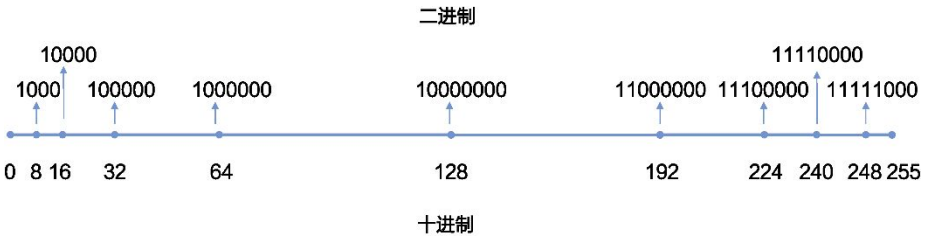


图3-1　二进制和十进制对应的关系

可以看到0～255共计256个数字，中间的数字就是128，128对应的二进制数就是1000 0000，这是一个分界点，128以前的二进制数最高位是0，128之后的二进制数的最高位都是1。

128～255中间的数，就是192，二进制是1100 0000。这就意味着从192开始的数，其二进制数最前面的两位都是1。

192～255中间的数，就是224，二进制是1110 0000。这就意味着从224开始的数，其二进制最前面的三位都是1。

通过这种方式很容易找出0～128的数64是二进制数100 0000对应的十进制数。0～64的数32就是二进制数10 0000对应的十进制数。

即便忘记了对应关系，只要画一条数轴，按照上述方法就能很快找到二进制和十进制的对应关系。

3.1.2 二进制数的规律

在后面学习合并网段时需要大家判断给出的几个子网是否能够合并成一个网段，需要能够写出一个数转换成二进制后的形式。下面就介绍一下二进制数的规律，如表3-1所示。本节介绍一个快速写出一个数的二进制形式的后几位的方法。

表3-1 二进制规律

十 进 制	二 进 制	十 进 制	二 进 制
0	0	11	1011
1	1	12	1100

十　进　制	二　进　制	十　进　制	二　进　制
2	10	13	1101
3	11	14	1110
4	100	15	1111
5	101	16	10000
6	110	17	10001

通过表3-1中的十进制和二进制的对应关系能找到以下规律。

- 能够被2整除的数，写成二进制形式，后一位是0。如果余数是1，则最后一位是1。
- 能够被4整除的数，写成二进制形式，后两位是00。如果余数是2，那就把2写成二进制，后两位是10。
- 能够被8整除的数，写成二进制形式，最后三位是000。如果余5，就把5写成二进制，后三位是101。
- 能够被16整除的数，写成二进制形式，最后四位是0000。如果余6，就把6写成二进制，最后四位是0110。
- 我们可以找出规律，如果让你写出一个十进制数转换成二进制数后后面的n位二进制数，可以将该数除以2^n，将余数写成n位二进制即可。

根据前面的规律，写出十进制数242转换成二进制数后的最后4位。

2^4是16，242除以16，余2，将余数写成4位二进制，就是0010。

3.2　理解IP地址

IP地址就是给每个连接在Internet上的主机分配的一个32位二进制地址。IP地址用来定位网络中的计算机和网络设备。

3.2.1　MAC地址和IP地址

计算机的网卡有物理层地址（MAC地址），为什么还需要IP地址呢？

如图3-2所示，网络中有3个网段，一个交换机对应一个网段，使用两个路由器来连接这3个网段。图中MA、MB、MC、MD、ME、MF以及M1、M2、M3和M4，分别代表计算机和路由器接口的MAC地址。

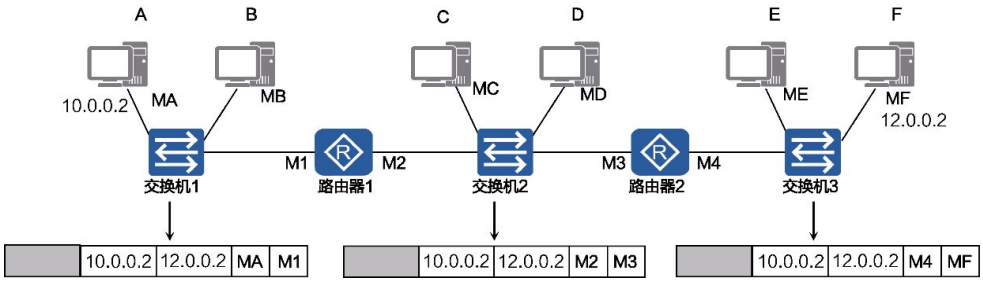


图3-2　MAC地址和IP地址的作用

假设计算机A给计算机F发送一个数据包，计算机A在网络层给数据包添加源IP地址（10.0.0.2）和目标IP地址（12.0.0.2）。

该数据包要想到达计算机F，要经过路由器1转发，该数据包如何才能让交换机1转发到路由器1呢？那就需要在数据链路层添加MAC地

址，源MAC地址为MA，目标MAC地址为M1。

路由器1收到该数据包，需要将该数据包转发到路由器2，这就要求将数据包重新封装成帧。帧的目标MAC地址是M3，源MAC地址是M2，这也要求重新计算帧校验序列。

数据包到达路由器2后需要重新封装，目标MAC地址为MF，源MAC地址为M4。交换机3将该帧转发给计算机F。

从图3-2可以看出，数据包的目标IP地址决定了数据包最终到达哪一个计算机，而目标MAC地址决定了该数据包下一跳由哪个设备接收，但不一定是终点。

如果全球计算机网络是一个大的以太网，那就不需要使用IP地址通信了，只使用MAC地址就可以了。大家想想那将是一个什么样的场景？一个计算机发广播帧，全球计算机都能收到，都要处理，整个网络的带宽将会被广播帧耗尽。所以还必须由网络设备路由器来隔绝以太网的广播，默认路由器不转发广播帧，路由器只负责在不同的网络间转发数据包。

3.2.2 IP地址的组成

在讲解IP地址之前，先介绍一下大家熟知的电话号码，通过电话号码来理解IP地址。

大家都知道，电话号码由区号和本地号码组成。如图3-3所示，石家庄地区的区号是0311，北京市的区号是010，保定地区的区号是0312。同一地区的电话号码有相同的区号，打本地电话不用拨区号，打长途才需要拨区号。

和电话号码一样，计算机的IP地址也由两部分组成，一部分为网络标识，一部分为主机标识，如图3-4所示，同一网段的计算机的IP地址的网络标识相同。路由器连接不同网段，负责不同网段之间的数据转发，交换机连接的则是同一网段的计算机。

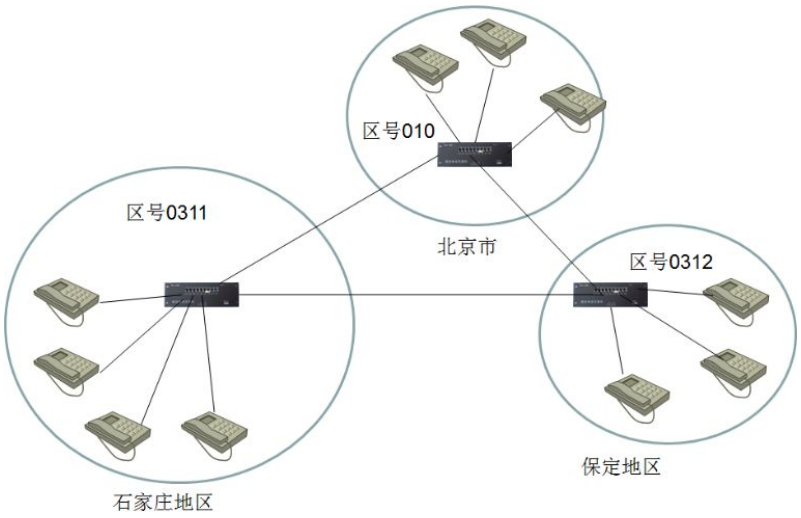


图3-3　区号和电话号

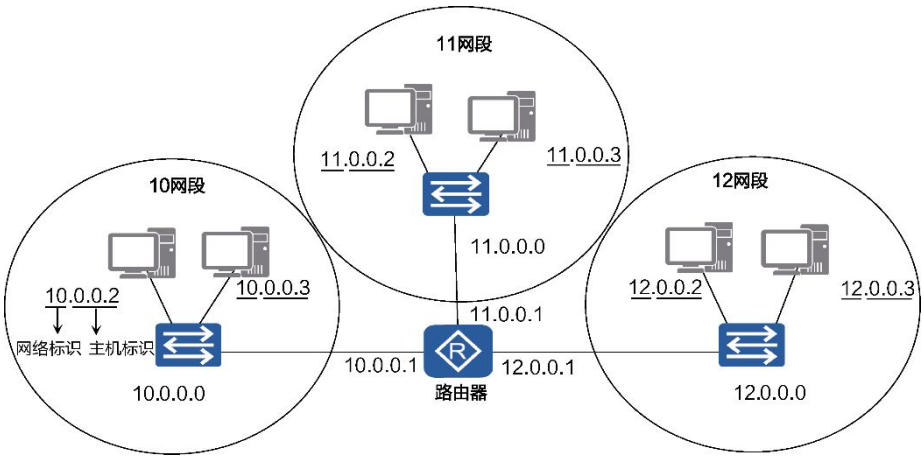


图3-4　网络标识和主机标识

计算机在和其他计算机通信之前，首先要判断目标IP地址和自己的IP地址是否在同一个网段，这决定了数据链路层的目标MAC地址是目标计算机的还是路由器接口的。

3.2.3　IP地址格式

按照TCP/IPv4协议栈规定，IP地址用32位二进制来表示，也就是32比特，换算成字节就是4字节。例如一个采用二进制形式的IP地址是“10101100000100000001111000111000”，这么长的地址，人们处理起来太费劲了。为了方便人们的使用，这些位被分割为4个部分，每一部分有8位，中间使用符号“.”分开。分成4部分的二进制IP地址10101100.00010000. 00011110.00111000经常被写成十进制的形式，于是，上面的IP地址可以表示为“172.16.30.56”。IP地址的这种表示法叫作“点分十进制表示法”，这显然比1和0的组合容易记忆得多。

点分十进制记法可以方便我们书写和记忆。计算机配置IP地址时就使用的这种写法，如图3-5所示。本书为了方便描述，给IP地址的这4部分进行了编号，从左到右分别称为第1部分、第2部分、第3部分和第4部分。

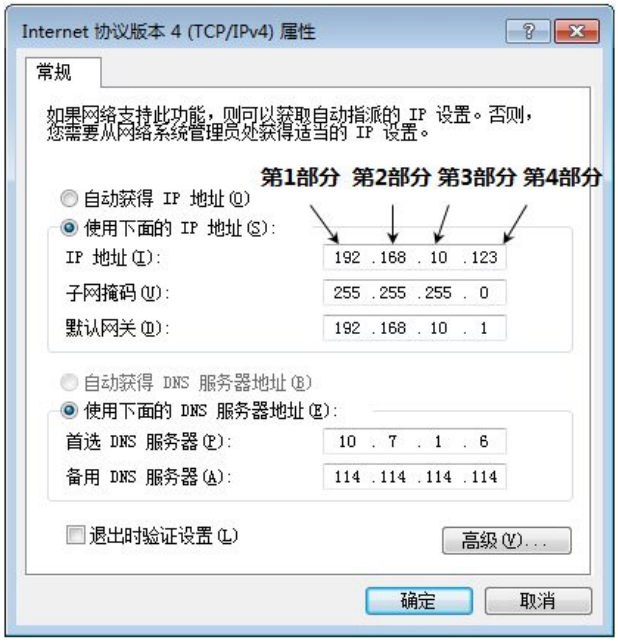


图3-5　点分十进制记法

8位二进制的11111111转换成十进制就是255，因此点分十进制的每一部分最大不能超过255。大家看到给计算机配置IP地址时，还会配置子网掩码和默认网关，下面就介绍子网掩码的作用。

3.2.4　子网掩码的作用

子网掩码（Subnet Mask）又叫子网掩码、地址掩码，它是一种用来指明一个IP地址的哪些位标识的是主机所在的子网以及哪些位标识

的是主机的位掩码。子网掩码只有一个作用，就是将某个IP地址划分成网络地址和主机地址两部分。

如图3-6所示，计算机的IP地址是131.107.41.6，子网掩码是255.255.255.0，所在网段是131.107.41.0，主机部分归零，这就是该主机所在的网段。该计算机和远程计算机通信，只要目标IP地址前面三部分是131.107.41就认为和该计算机在同一个网段，比如该计算机和IP地址131.107.41.123在同一个网段，和IP地址131.107.42.123不在同一个网段，因为网络部分不相同。

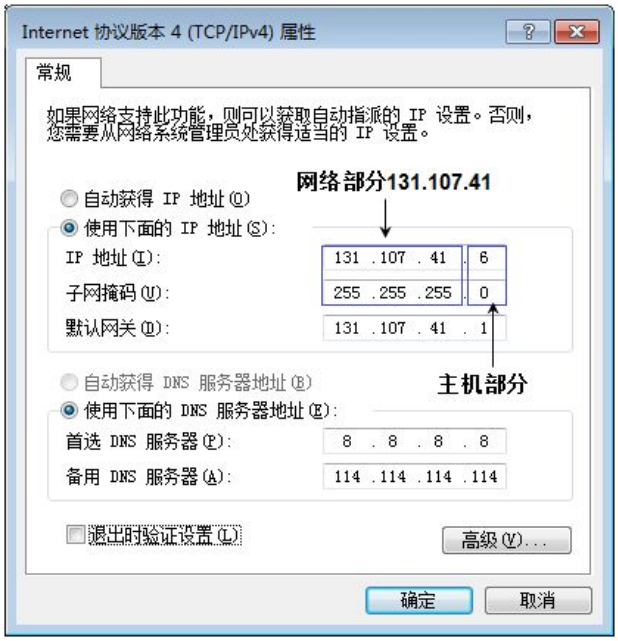


图3-6　子网掩码的作用（一）

如图3-7所示，计算机的IP地址是131.107.41.6，子网掩码是255.255.0.0，计算机所在网段是131.107.0.0。该计算机和远程计算机通信，目标IP地址只要前面两部分是131.107就认为和该计算机在同

一个网段，比如该计算机和IP地址131.107.42.123在同一个网段，而和IP地址131.108.42.123不在同一个网段，因为网络部分不同。

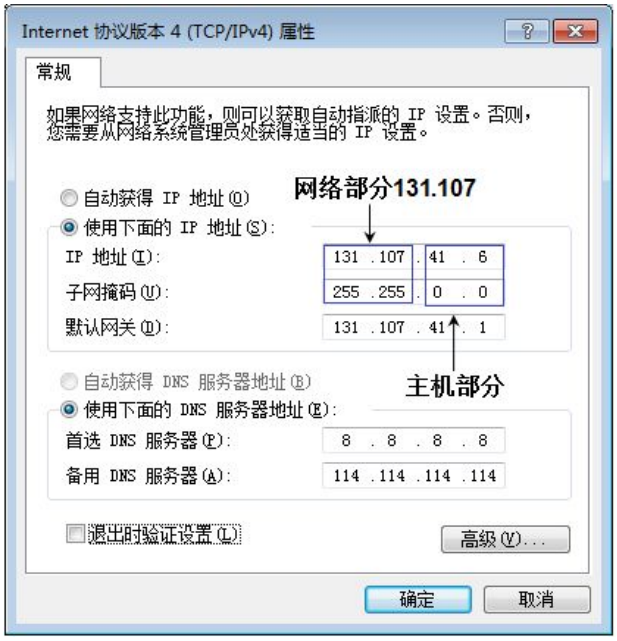


图3-7　子网掩码的作用（二）

如图3-8所示，计算机的IP地址是131.107.41.6，子网掩码是255.0.0.0，计算机所在网段是131.0.0.0。该计算机和远程计算机通信，目标IP地址只要第1部分是131就认为和该计算机在同一个网段。比如该计算机和IP地址131.108.42.123在同一个网段，而和IP地址132.108.42.123不在同一个网段，因为网络部分不同。

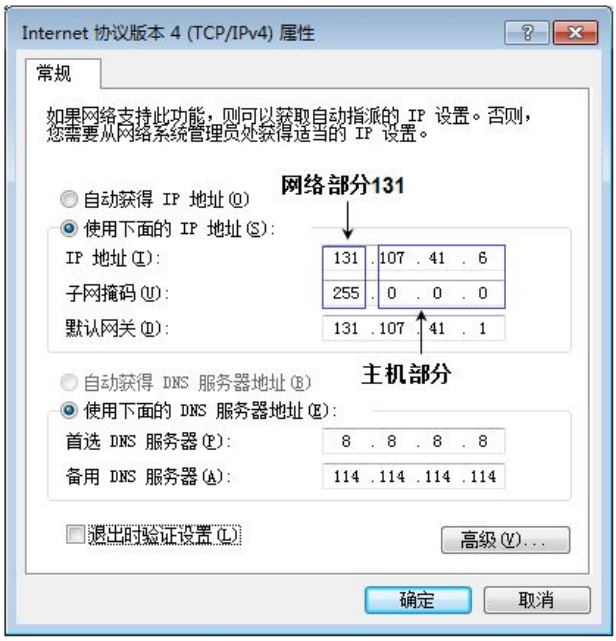


图3-8　子网掩码的作用（三）

计算机如何使用子网掩码来计算自己所在的网段呢？

如图3-9所示，如果一台计算机的IP地址配置为131.107.41.6，子网掩码为255.255.255.0。将其IP地址和子网掩码都写成二进制，对应的二进制位进行“与”运算。两个都是1才得1，否则都得0，即1和1做“与”运算得1，0和1或1和0做“与”运算都得0，0和0做“与”运算得0。这样将IP地址和子网掩码做完“与”运算后，主机位不管是什么值都归零，网络位的值保持不变，得到该计算机所处的网段为131.107.41.0。

IP地址			131							107							41							6							
二进制IP地址	1	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1	1	0
	与	与																														
子网掩码			255							255							255							0							
二进制网络掩码	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
地址和网络掩码做"与"运算	↓	↓																														
网络号			131							107							41							0							
二进制网络号	1	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0

图3-9　子网掩码的作用（四）

子网掩码很重要，配置错误会造成计算机通信故障。计算机和其他计算机通信时，首先需要判断目标地址和自己是否在同一个网段，先用自己的子网掩码和自己的IP地址进行“与”运算得到自己所在的网段，再用自己的子网掩码和目标地址进行“与”运算，看看得到网络部分与自己所在网段是否相同。如果不相同，则不在同一个网段，封装帧时目标MAC地址用网关的MAC地址，交换机将帧转发给路由器接口；如果相同，则直接使用目标IP地址的MAC地址封装帧，直接把帧发给目标IP地址。

如图3-10所示，路由器连接两个网段131.107.41.0 255.255.255.0和131.107.42.0 255.255. 255.0，同一个网段中的计算机子网掩码相同，计算机的网关就是到其他网段的出口，也就是路由器接口地址。路由器接口使用的地址可以是本网段中任何一个地址，不过通常使用该网段第一个可用的地址或最后一个可用的地址，这是为了尽可能避免和网络中的其他计算机地址冲突。

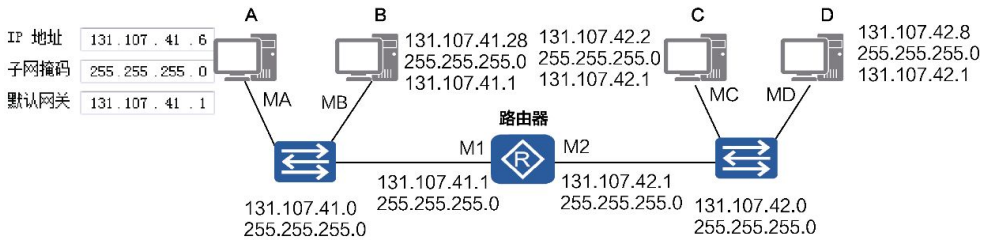


图3-10　子网掩码和网关的作用

如果计算机没有设置网关，那么跨网段通信时它就不知道谁是路由器，下一跳该给哪个设备。因此计算机要想实现跨网段通信，必须

指定网关。

如图3-11所示，连接在交换机上的计算机A和计算机B的子网掩码设置不一样，都没有设置网关。思考一下，计算机A是否能够和计算机B通信？只有数据包能去能回网络才能通。

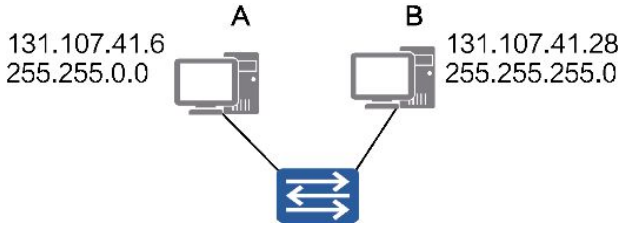


图3-11　子网掩码设置不一样（一）

计算机A和自己的子网掩码做“与”运算，得到自己所在的网段131.107.0.0，目标地址131.107.41.28也属于131.107.0.0网段，计算机A把帧直接发送给计算机B。计算机B给计算机A发送返回的数据包，计算机B在131.107.41.0网段，目标地址131.107.41.6也属于131.107.41.0网段，所以计算机B也能够把数据包直接发送到计算机A，因此计算机A能够和计算机B通信。

如图3-12所示，连接在交换机上的计算机A和计算机B的子网掩码设置不一样，IP地址如图3-12所示，都没有设置网关。思考一下，计算机A是否能够和计算机B通信？

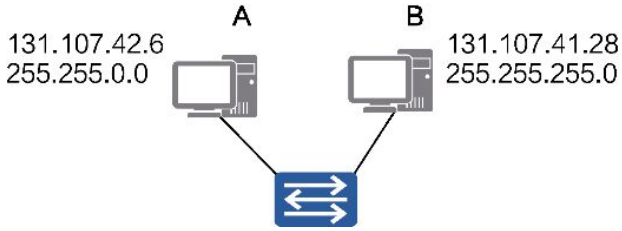


图3-12　子网掩码设置不一样（二）

计算机A和自己的子网掩码做“与”运算，得到自己所在的网段131.107.0.0，目标地址131.107.41.28也属于131.107.0.0网段，计算机A可以把数据包发送给计算机B。计算机B给计算机A发送返回的数据包，计算机B使用自己的子网掩码计算自己所属网段，得到自己所在的网段为131.107.41.0，目标地址131.107.42.6不属于131.107.41.0网段，计算机B没有设置网关，不能把数据包发送到计算机A，因此计算机A能发送数据包给计算机B，但是计算机B不能发送返回的数据包，因此网络不通。

3.2.5　子网掩码的另一种表示方法

IP地址有“类”的概念，A类地址默认子网掩码为255.0.0.0，B类地址默认子网掩码为255.255.0.0、C类地址默认子网掩码为255.255.255.0。等长子网划分和变长子网划分打破了IP地址“类”的概念，子网掩码也打破了字节的限制，这种子网掩码被称为可变长子网掩码（Variable Length Subnet Masking，VLSM）。为了方便表示可变长子网掩码，子网掩码还有另一种写法。比如131.107.23.32/25、192.168.0.178/26，反斜杠后面的数字表示将子网掩码写成二进制形式后1的个数。

这种方式打破了IP地址“类”的概念，使得Internet服务提供商（ISP）可以灵活地将大的地址块分成恰当的小地址块（子网）给客户，不会造成大量IP地址浪费。这种方式也可以使得Internet上的路

由器路由表大大精简。这种方式叫作无类域间路由（Classless Inter-Domain Routing，CIDR），子网掩码中1的个数被称为CIDR值。

CIDR的作用就是支持IP地址的无类规划，CIDR采用13～27位可变网络ID，而不是A、B、C类网络ID所用的固定的8、16和24位。在IP地址后面添加一个“/”，后面是二进制子网掩码的位数。比如192.168.10.32/24，意味着该地址子网掩码长度为24，即11111111.11111111. 11111111. 00000000，等价于子网掩码255.255.255.0。

3.3　IP地址详解

3.3.1　IP地址分类

最初设计互联网络时，Internet委员会定义了5种IP地址类型以适合不同容量的网络，即A类～E类。其中A、B、C三类由InternetNIC在全球范围内统一分配，D、E类为特殊地址。

IPv4地址共32位二进制，分为网络ID和主机ID。哪些位是网络ID、哪些位是主机ID，最初是使用IP地址第1部分进行标识的。也就是说只要看到IP 地址的第1部分就知道该地址的子网掩码。这种方式将IP地址分成了A类、B类、C类、D类和E类5类。

如图3-13所示，网络地址最高位是0的地址为A类地址。网络ID全0时不能用，127作为保留网段，因此A类地址的第1部分取值范围为1～126。

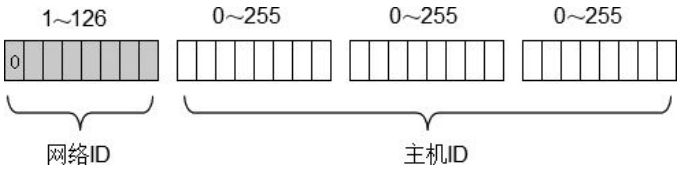


图3-13　A类地址网络位和主机位

A类网络的默认子网掩码为255.0.0.0。主机ID由第2部分、第3部分和第4部分组成，每部分的取值范围为0～255，共256种取值。学过排列组合就会知道，一个A类网络主机的数量是

256×256×256=16777216，取值范围是0～16777215，0也算一个数。可用的地址还需减去2，主机ID全0的地址为网络地址，不能给计算机使用，而主机ID全1的地址为广播地址，也不能给计算机使用，因此可用的地址数量为16777214。如果给主机ID全1的地址发送数据包，那么计算机产生一个广播帧，然后发送到本网段全部计算机。

如图3-14所示，网络地址最高位是10的地址为B类地址。IP地址第1部分的取值范围为128～191。

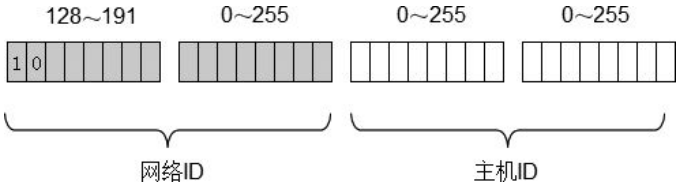


图3-14　B类地址网络位和主机位

B类网络的默认子网掩码为255.255.0.0。主机ID由第3部分和第4部分组成，每个B类网络可以容纳的最大主机数量为256×256=65536，取值范围为0～65535，去掉主机位全0和全1的地址，可用的地址数量为65534个。

如图3-15所示，网络地址最高位是110的地址为C类地址。IP地址第1部分的取值范围为192～223。

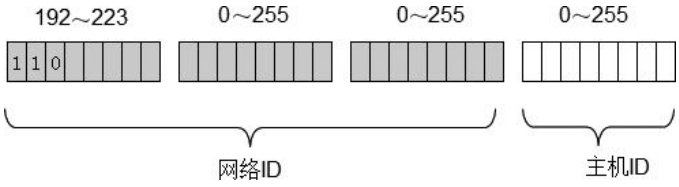


图3-15　C类地址网络位和主机位

C类网络的默认子网掩码为255.255. 255.0。主机ID由第4部分组成，每个C类的网络地址数量为256，取值范围0～255，去掉主机位全0和全1的地址，可用地址数量为254。

如图3-16所示，网络地址最高位是1110的地址为D类地址。D类地址第1部分的取值范围为224～239。D类地址是用于多播（也称为组播）的地址，多播地址没有子网掩码。希望读者能够记住多播地址的范围，因为有些病毒除了在网络中发送广播外，还有可能发送多播数据包。当你使用抓包工具排除网络故障时，必须能够断定捕获的数据包是多播还是广播。

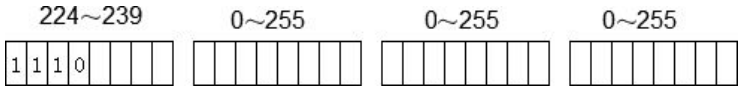


图3-16　D类地址

如图3-17所示，网络地址最高位是11110的地址为E类地址。第1部分的取值范围为240～254，保留为今后使用。本书并不讨论这两个类型的地址（并且也不要求你了解这些内容）。

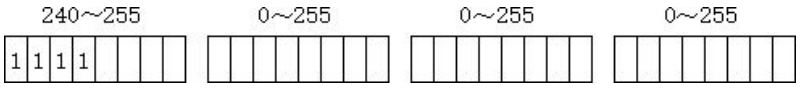


图3-17　E类地址

为了方便大家记忆，请观察图3-18，将IP地址的第1部分画为一条数轴，数值范围从0～255。A类地址、B类地址、C类地址、D类地址以及E类地址的取值范围，一目了然。

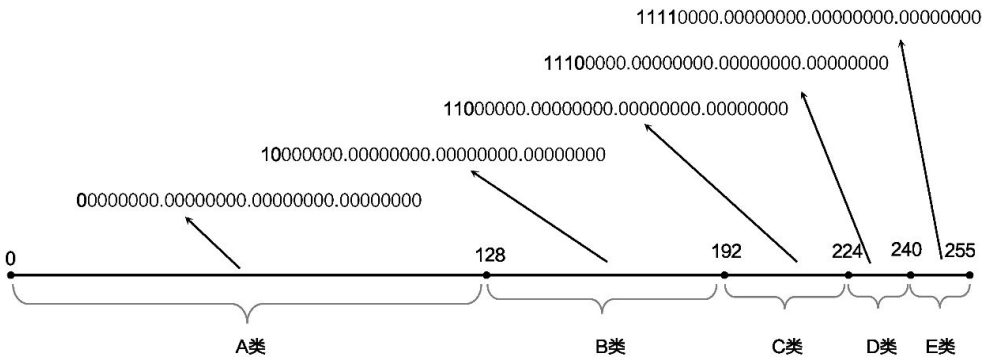


图3-18　IP地址分类助记图

3.3.2　特殊的IP地址

有些IP地址被保留用于某些特殊目的，网络管理员不能将这些地址分配给计算机。下面列出了这些被排除在外的地址，并说明为什么要保留它们。

- 主机ID全为0的地址：特指某个网段，比如192.168.10.0、255.255.255.0。
- 主机ID全为1的地址：特指该网段的全部主机，如果你的计算机发送数据包时使用的是主机ID全是1的IP地址，那么数据链路层地址用广播地址FF-FF-FF-FF-FF-FF。比如你的计算机IP地址是192.168.10.10，子网掩码是255.255.255.0，它要发送一个广播包，目标IP地址是192.168.10.255，帧的目标MAC地址是FF-FF-FF-FF-FF-FF，那么该网段中全部计算机都能收到。
- 127.0.0.1：回送地址，指本机地址，一般用作测试使用。回送地址（127.x.x.x）即本机回送地址（Loopback Address），指主机IP堆栈内部的IP地址，主要用于网络软件测试以及本地计算机进程间通信。无论什么程序，一旦使用回送地址发送数据，协议软件立即返回，不进行任何网络传输。任何计算机都可以用该地址

访问自己的共享资源或网站，如果ping 该地址能够通，说明你的计算机的TCP/IP协议栈工作正常，即便你的计算机没有网卡，ping 127.0.0.1还是能够通的。

- 169.254.0.0：169.254.0.0～169.254.255.255实际上是自动私有IP地址。在Windows 2000以前的操作系统中，如果计算机无法获取IP地址，则自动配置成“IP地址：0.0.0.0”“子网掩码：0.0.0.0”的形式，导致其不能与其他计算机通信。而对于Windows 2000以后的操作系统，则在无法获取IP地址时自动配置成“IP地址：169.254.×.×”“子网掩码：255.255.0.0”的形式，这样可以使所有获取不到IP地址的计算机之间能够通信，如图3-19和图3-20所示。

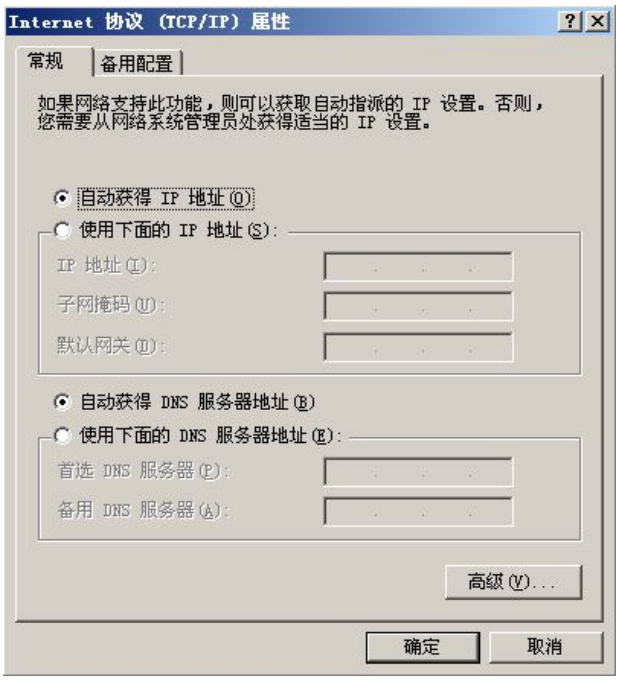


图3-19　自动获得地址

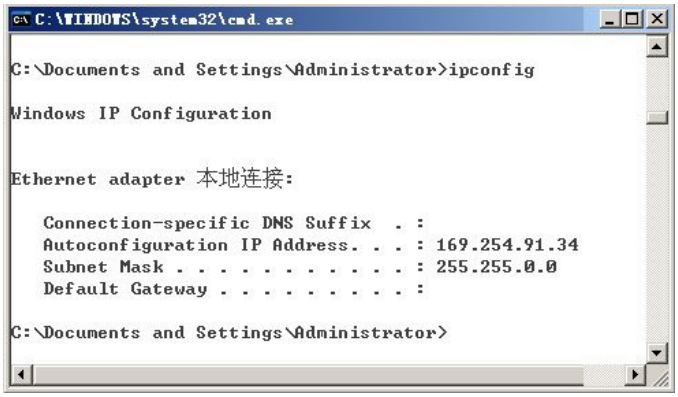


图3-20　Windows自动配置的IP地址

- 0.0.0.0：如果计算机的IP地址和网络中的其他计算机地址冲突，那么使用ipconfig命令看到的就是0.0.0.0，子网掩码也是0.0.0.0，如图3-21所示。

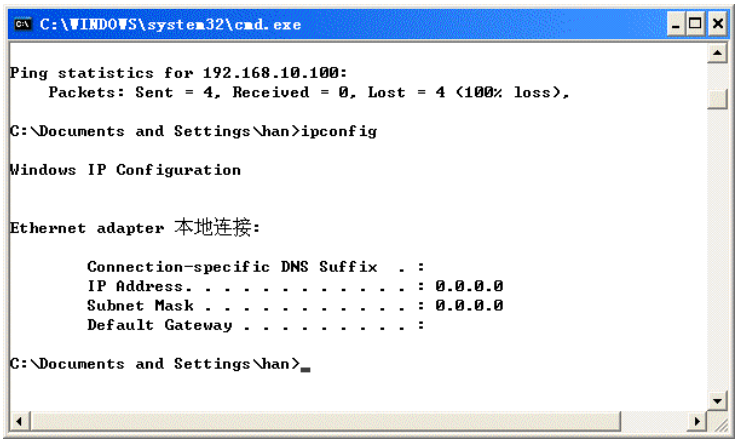


图3-21　地址冲突

3.4　私网地址和公网地址

从事网络方面的工作必须了解公网IP地址和私网IP地址，下面就给大家进行详细讲解。

3.4.1　公网地址

在Internet网络上有千百万台主机，都需要使用IP地址进行通信，这就要求接入Internet的各个国家的各级ISP使用的IP地址块不能重叠，这需要互联网有一个组织进行统一的地址规划和分配。这些统一规划和分配的全球唯一的地址被称为“公网地址”（public address）。

公网地址的分配和管理由因特网信息中心（Internet Network Information Center，InterNIC）负责。各级ISP使用的公网地址都需要向InterNIC提出申请，由InterNIC统一发放，这样就能确保地址块不冲突。

正是因为IP地址是统一规划、统一分配的，所以我们只要知道IP地址，就能很方便地查到该地址是哪个城市的哪个ISP。如果你的网站遭到了来自某个地址的攻击，通过以下方式就可以知道攻击者所在的城市和所属的运营商。

比如我们想知道淘宝网站位于哪个城市哪个ISP的机房。那么需要先解析出网站的IP地址，在用命令提示符ping该网站的域名，就能解

析出该网站的IP地址。

如图3-22所示，在百度查找淘宝网站IP地址所属运营商和所在位置。



图3-22　查看淘宝网站IP地址所属运营商和所在地

3.4.2　私网地址

创建IP寻址方案的人也创建了私网IP地址，这些地址可以被用于私有网络。Internet上没有这些IP地址，Internet上的路由器也没有到私有网络的路由。在Internet上不能访问这些私网地址，从这一点来说使用私网地址的计算机更加安全，同时也有效地节省了公网IP地址。

保留的私有IP地址如下所列。

- A类：10.0.0.0 255.0.0.0，保留了一个A类网络。

- B类：172.16.0.0 255.255.0.0～172.31.0.0 255.255.0.0，保留了16个B类网络。
- C类：192.168.0.0 255.255.255.0～192.168.255.0 255.255.255.0，保留了256个C类网络。

如果你负责为一个公司规划网络，那么到底使用哪一类私有地址呢？如果公司目前有7个部门，每个部门不超过200台计算机，你可以考虑使用保留的C类私有地址；如果你为石家庄市教委规划网络，石家庄市教委要和石家庄地区的几百所中小学的网络连接，网络规模较大，那就选择保留的A类私有网络地址，最好用10.0.0.0网络地址并带有/24的子网掩码，这样可以有65536个网络供你使用，并且每个网络都允许带有254台主机，这样会给学校留有非常大的地址空间。

3.5　子网划分

3.5.1　为什么需要子网划分

现在在Internet上使用的协议是TCP/IP第4版，也就是IPv4，其IP地址由32位的二进制数组成，这些地址如果全部能分配给计算机，共计2^{32} = 4294967296，大约40亿个可用地址，这些地址去除掉D类地址和E类地址，还有保留的私网地址后，能够在Internet上使用的公网地址就变得越发紧张。并且我们每个人需要使用的地址也不止1个，现在智能手机、智能家电接入互联网都需要IP地址。

在IPv6还没有完全在互联网普遍应用的IPv4和IPv6共存阶段，IPv4公网地址资源日益紧张，这就需要用到本章讲到的子网划分技术，使得IP地址能够充分利用，减少地址浪费。

如图 3-23 所示，按照IP地址传统的分类方法，一个网段有200个计算机，分配一个C类网络212.2.3.0 255.255.255.0，可用的地址范围为212.2.3.1～212.2.5.254，尽管没有全部用完，但这种情况还不算是极大浪费。

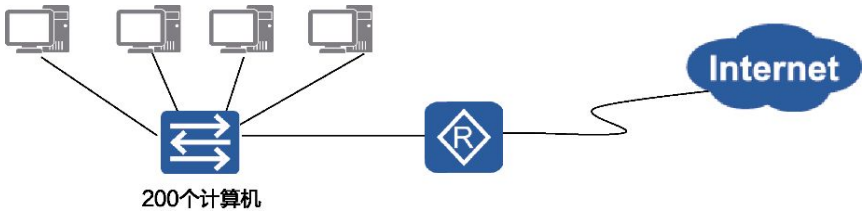


图3-23　地址浪费的情况

如果一个网络中有400台计算机，分配一个C类网络，地址就不够用了，那就分配一个B类网络131.107.0.0 255.255.0.0，该B类网络可用的地址范围为131.107.0.1～131.107.255.254，一共有65534个地址可用，这就造成了极大浪费。

下面讲的子网划分，就是要打破IP地址的分类所限定的地址块，使得IP地址的数量和网络中的计算机数量更加匹配。由简单到复杂，我们先讲等长子网划分，再讲变长子网划分。

3.5.2　等长子网划分

等长子网划分就是将一个网段等分成多个网段，也就是等分成多个子网。

子网划分就是借用现有网段的主机位做子网位，划分出多个子网。子网划分的任务包括两部分：

- 确定子网掩码的长度；
- 确定子网中第一个可用的IP地址和最后一个可用的IP地址。

等长子网划分就是将一个网段等分成多个网段。

1. 等分成两个子网

下面以一个C类网络划分为两个子网为例，讲解子网划分的过程。

如图3-24所示，某公司有两个部门，每个部门有100台计算机，都通过路由器连接Internet。给这200台计算机分配一个C类网络192.168.0.0，该网段的子网掩码为255.255.255.0，连接局域网的路由器接口使用该网段的第一个可用的IP地址192.168.0.1。

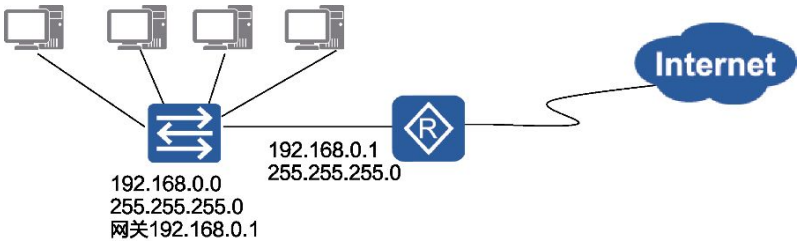


图3-24　一个网段的情况

为了安全考虑，我们打算将这两个部门的计算机分为两个网段，中间使用路由器隔开。计算机数量没有增加，还是200台，因此一个C类网络的IP地址是足够用的。现在将192.168.0.0 255.255.255.0这个C类网络划分成两个子网。

如图3-25所示，将IP地址的第4部分写成二进制形式，子网掩码使用两种方式表示：二进制和十进制。子网掩码往右移一位，这样C类地址主机ID的第1位就成为网络位，该位为0是A子网，该位为1是B子网。

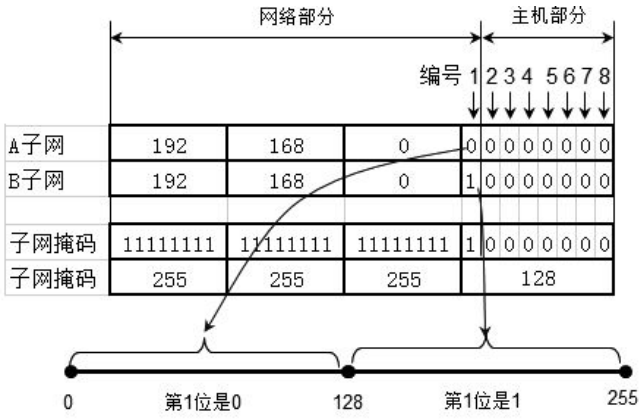


图3-25　等分成两个子网

如图3-25所示，IP地址的第4部分，其值在0到127之间的，第1位均为0；其值在128到255之间的，第1位均为1。这样，原来的网络分成了A、B两个子网，以128为界。现在的子网掩码中的1变成了25个，写成十进制就是255.255.255.128。子网掩码向后移动了1位（即子网掩码中1的数量增加1），就划分出2个子网。

A和B两个子网的子网掩码都为255.255.255.128。

A子网可用的地址范围为192.168.0.1～192.168.0.126，IP地址为192.168.0.0。由于主机位全为0，所以不能分配给计算机使用。如图3-26所示，192.168.0.127由于主机位全为1，也不能分配计算机。



图3-26　网络部分和主机部分

B子网可用的地址范围为192.168.0.129～192.168.0.254。IP地址192.168.0.128由于主机位全为0，所以不能分配给计算机使用；IP地址192.168.0.255由于主机位全为1，也不能分配给计算机。

划分成两个子网后的网络规划如图3-27所示。

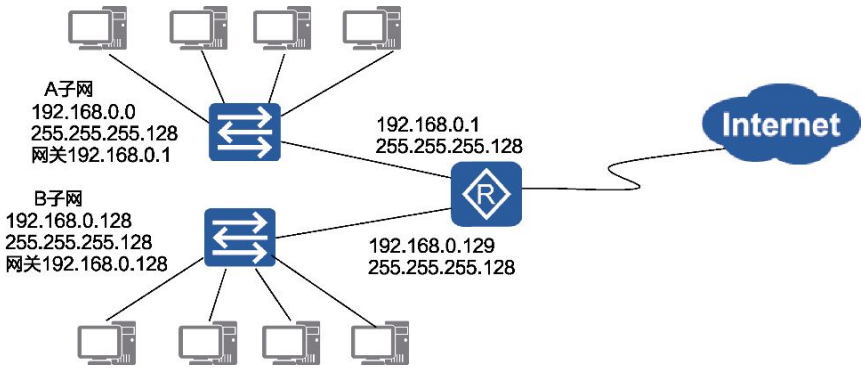


图3-27　划分子网后的地址规划

2. 等分成4个子网

假如公司有4个部门，每个部门有50台计算机，现在使用192.168.0.0/24这个C类网络。从安全方面考虑，我打算将每个部门的计算机放置到独立的网段中，这就要求将192.168.0.0 255.255.255.0这个C类网络划分为4个子网，那么如何划分成4个子网呢？

如图3-28所示，将192.168.0.0 255.255.255.0网段的IP地址的第4部分写成二进制，要想分成4个子网，需要将子网掩码往右移动两位，这样第1位和第2位就变为网络位。这就可以分成4个子网，第1位和第2位为00是A子网，为01是B子网，为10是C子网，为11是D子网。

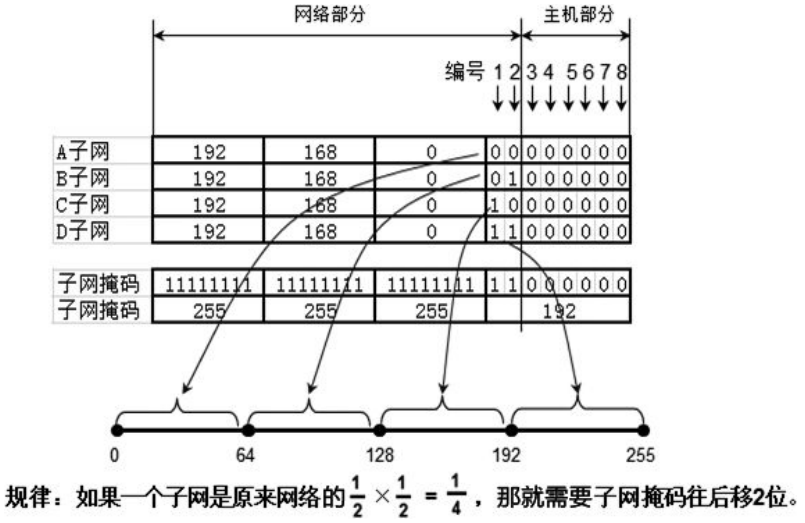


图3-28　等分为4个子网

A、B、C、D子网的子网掩码都为255.255.255.192。

A子网可用的开始地址和结束地址为192.168.0.1～192.168.0.62。

B子网可用的开始地址和结束地址为192.168.0.65～192.168.0.126。

C子网可用的开始地址和结束地址为192.168.0.129～192.168.0.190。

D子网可用的开始地址和结束地址为192.168.0.193～192.168.0.254。

注意：如图3-29所示，每个子网的最后一个地址都是本子网的广播地址，不能分配给计算机使用，如A子网的63、B子网的127、C子网的191和D子网的255。



图3-29　网络部分和主机部分

3．等分为8个子网

如果想把一个C类网络等分成8个子网，如图3-30所示，那么子网掩码需要往右移3位，这样才能划分出8个子网。第1位、第2位和第3位都变成网络位。

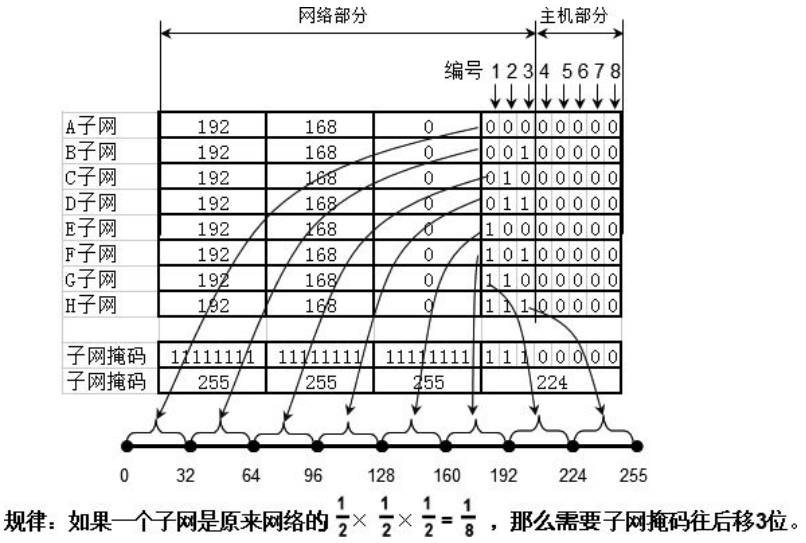


图3-30　等分成8个子网

每个子网的子网掩码都一样，为255.255.255.224。

A子网可用的开始地址和结束地址为192.168.0.1～192.168.0.30。

B子网可用的开始地址和结束地址为192.168.0.33～192.168.0.62。

C子网可用的开始地址和结束地址为192.168.0.65～192.168.0.94。

D子网可用的开始地址和结束地址为192.168.0.97～192.168.0.126。

E子网可用的开始地址和结束地址为192.168.0.129～192.168.0.158。

F子网可用的开始地址和结束地址为192.168.0.161～192.168.0.190。

G子网可用的开始地址和结束地址为192.168.0.193～192.168.0.222。

H子网可用的开始地址和结束地址为192.168.0.225～192.168.0.254。

注意：每个子网能用的主机IP地址，都要去掉主机位全为0和主机位全为1的地址。31、63、95、127、159、191、223、255都是相应子网的广播地址。

每个子网是原来的$\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2}$，即3个$\frac{1}{2}$，子网掩码往右移3位。

总结：如果一个子网地址块是原来网段的$\left(\frac{1}{2}\right)^n$，那么子网掩码就在原网段的基础上后移$n$位。

3.5.3 等长子网划分示例

上一节使用一个C类网络讲解了等长子网划分，总结的规律照样也适用于B类网络的子网划分。在不太熟悉的情况下容易出错，最好将主机位写成二进制的形式，确定子网掩码和每个子网第一个和最后一个能用的地址。

如图3-31所示，将131.107.0.0 255.255.0.0等分成2个子网。子网掩码往右移动1位，就能等分成两个子网。



图3-31 B类网络的子网划分

这两个子网的子网掩码都是255.255.128.0。

先确定A子网的第一个可用地址和最后一个可用地址，大家在不熟悉的情况下最好按照图3-32的形式将主机部分写成二进制，主机位不

能全是0，也不能全是1，然后再根据二进制写出第一个可用地址和最后一个可用地址。



图3-32　A子网地址范围

A子网的第一个可用地址是131.107.0.1，最后一个可用地址是131.107.127.254。大家思考一下，A子网中的131.107.0.255这个地址是否可以给计算机使用？

如图 3-33 所示，B 子网的第一个可用地址是 131.107.128.1，最后一个可用地址是131.107.255.254。

这种方式虽然步骤烦琐一点，但不容易出错，等熟悉了之后就可以直接写出子网的第一个可用地址和最后一个可用地址了。



图3-33　B子网地址范围

前面给大家讲的都是将一个网段等分成多个子网。如果每个子网中计算机的数量不一样，就需要将该网段划分成地址空间不等的子

网，这就是变长子网划分。有了等长子网划分的基础，划分变长子网也就容易了。

3.5.4　变长子网划分

如图3-34所示，有一个C类网络192.168.0.0 255.255.255.0，需要将该网络划分成5个网段以满足以下网络需求：该网络中有3个交换机，分别连接20台计算机、50台计算机和100台计算机，路由器之间的连接接口也需要地址，这两个地址也是一个网段，这样网络中一共有5个网段。

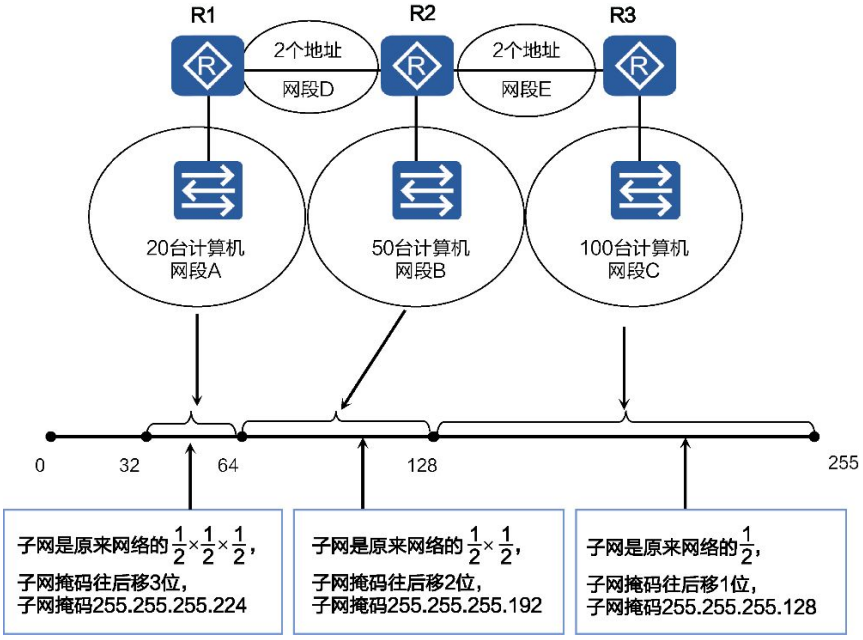


图3-34　变长子网划分

如图3-34所示，将192.168.0.0 255.255.255.0的主机位从0～255画一条数轴，将128～255的地址空间给100台计算机的网段比较合适，该子网的地址范围是原来网络的$\frac{1}{2}$，子网掩码往后移1位，写成十进制形式就是255.255.255.128。第一个能用的地址是192.168.0.129，最后一个能用的地址是192.168.0.254。

64～127的地址空间给50台计算机的网段比较合适，该子网的地址范围是原来的$\frac{1}{2} \times \frac{1}{2}$，子网掩码往后移2位，写成十进制就是255.255.255.192。第一个能用的地址是192.168.0.65，最后一个能用的地址是192.168.0.126。

32～63的地址空间给20台计算机的网段比较合适，该子网的地址范围是原来的$\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2}$，子网掩码往后移3位，写成十进制就是255.255.255.224。第一个能用的地址是192.168.0.33，最后一个能用的地址是192.168.0.62。

当然我们也可以使用以下的子网划分方案，100台计算机的网段可以使用0～127的子网，50台计算机的网段可以使用128～191的子网，20台计算机的网段可以使用192～223的子网，如图3-35所示。

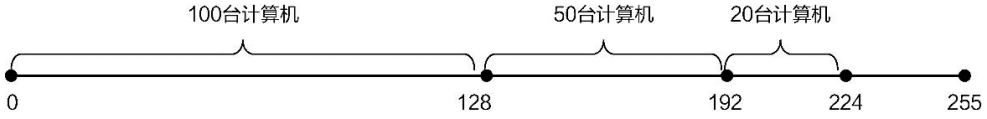


图3-35　子网划分数轴

规律：如果一个子网地址块是原来网段的$\left(\frac{1}{2}\right)^n$，子网掩码就在原网段的基础上后移$n$位，不等长子网的子网掩码也不同。

3.5.5　点到点网络的子网掩码

如果某个网络中就需要两个IP地址，那么子网掩码该是多少呢？如图3-34所示，路由器之间连接的接口也是一个网段，且只需要两个地址。下面看看如何给图3-34中的D网络和E网络规划子网。

如图3-36所示，0～3的子网可以给D网络中的两个路由器接口，第一个可用的地址是192.168.0.1，最后一个可用的地址是192.158.0.2，192.168.0.3是该网络中的广播地址。



图3-36　广播地址

4～7的子网可以给E网络中的两个路由器接口，第一个可用的地址是192.168.0.5，最后一个可用的地址是192.158.0.6，192.168.0.7是该网络中的广播地址，如图3-37所示。

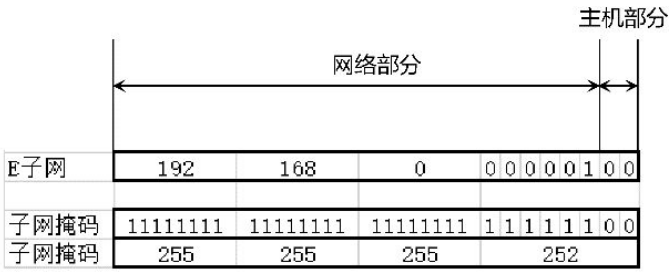


图3-37　广播地址

每个子网是原来网络的$\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}$，也就是$\left(\frac{1}{2}\right)^6$，子网掩码向后移动6位，11111111.11111111.11111111.11111100写成十进制也就是255.255.255.252。

子网划分的最终结果如图3-38所示。经过精心规划，该方案不但满足了5个网段的地址需求，还剩余了两个地址块，8～16地址块和16～32地址块没有被使用。

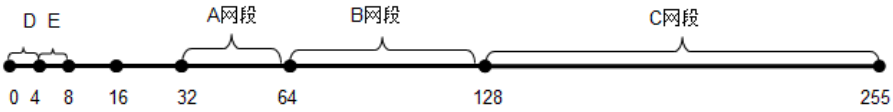


图3-38　分配的子网和剩余的子网

3.5.6　判断IP地址所属的网段

下面来学习根据给出的IP地址和子网掩码判断该IP地址所属的网段。前面说过，将IP地址中的主机位归0，此时的地址就是该主机所在的网段。

判断192.168.0.101/26所属的子网。

该地址为C类地址，默认子网掩码为24位，现在是26位。子网掩码往右移了两位，根据以上总结的规律，每个子网是原来的$\frac{1}{2}\times\frac{1}{2}$，即将这个C类网络等分成了4个子网。如图3-39所示，101所处的位置位于64～128，主机位归0后等于64，因此该地址所属的子网是192.168.0.64。

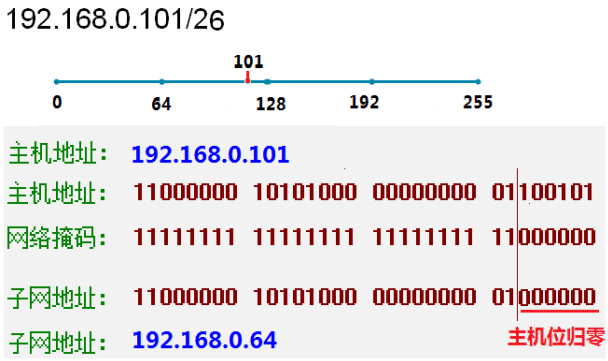


图3-39　判断地址所属子网（一）

判断192.168.0.101/27所属的子网。

该地址为C类地址，默认子网掩码为24位，现在是27位。子网掩码往右移了3位，根据以上总结的规律，每个子网是原来的$\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}$，即将这个C类网络等分成8个子网。如图3-40所示，101所处的位置位于96～128，主机位归0后等于96。因此该地址所属的子网是192.168.0.96。

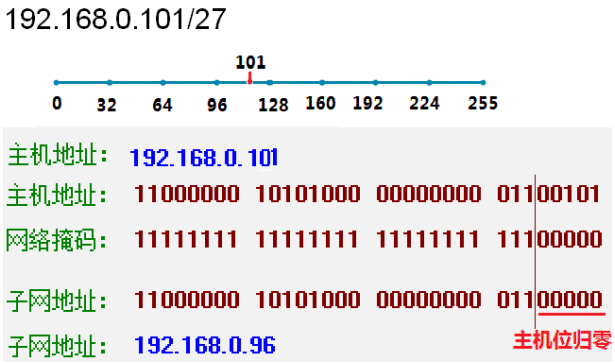


图3-40　判断地址所属子网（二）

总结如下：

IP地址192.168.0.0～192.168.0.63都属于192.168.0.0/26子网；

IP地址192.168.0.64～192.168.0.127都属于192.168.0.64/26子网；

IP地址192.168.0.128～192.168.0.191都属于192.168.0.128/26子网；

IP地址192.168.0.192～192.168.0.255都属于192.168.0.192/26子网，如图3-41所示。

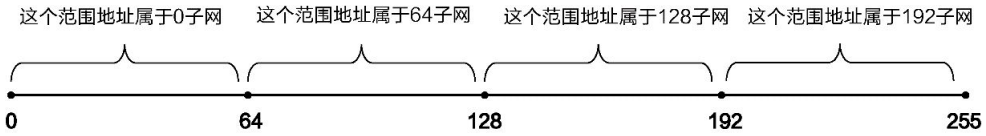


图3-41　断定IP地址所属子网的规律

3.5.7　子网划分需要注意的几个问题

- 将一个网络等分成两个子网，每个子网肯定是原来网络的一半。

比如将192.168.0.0/24分成两个子网，要求一个子网能够放140台主机，另一个子网放60台主机，能实现吗？

从主机数量来说，总数没有超过254台，该C类网络能够容纳这些地址，但划分成两个子网后却发现，这140台主机在这两个子网中都不能容纳，如图3-42所示，因此不能实现。140台主机最少占用一个C类地址。

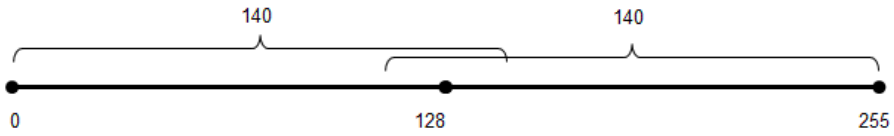


图3-42　子网地址不能交叉

- 子网地址不可重叠。

如果将一个网络划分多个子网，这些子网的地址空间不能重叠。

将192.168.0.0/24划分成3个子网，子网A 192.168.0.0/25、子网C 192.168.0.64/26和子网B 192.168.0.128/25，这就出现了地址重叠，如图3-43所示，子网A和子网C的地址重叠了。

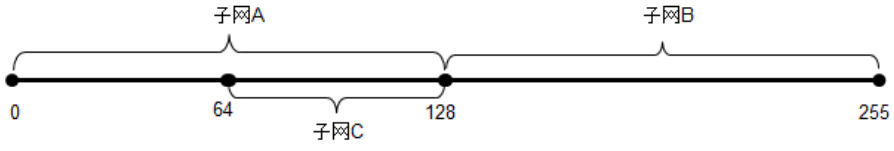


图3-43　子网地址不能重叠

3.6　合并网段

前面讲解的子网划分，就是将一个网络的主机位当作网络位来划分出多个子网。也可以将多个网段合并成一个大的网段，合并后的网段称为超网，下面介绍合并网段的方法。

3.6.1　合并网段的方法

如图3-44所示，某企业有一个网段，该网段有200台计算机，使用192.168.0.0 255.255.255.0网段，后来计算机数量增加到400台。

在该网络中添加交换机，可以扩展网络的规模。一个C类IP地址不够用，再添加一个C类地址192.168.1.0 255.255.255.0。这些计算机物理上在一个网段，但是IP地址没在一个网段，即逻辑上不在一个网段。如果想让这些计算机之间能够通信，可以在路由器的接口添加这两个C类网络的地址作为这两个网段的网关。

在这种情况下，A计算机与B计算机进行通信，必须通过路由器转发，这样两个子网才能够通信。本来这些计算机物理上在同一个网段，但还需要路由器转发，可见效率不高。

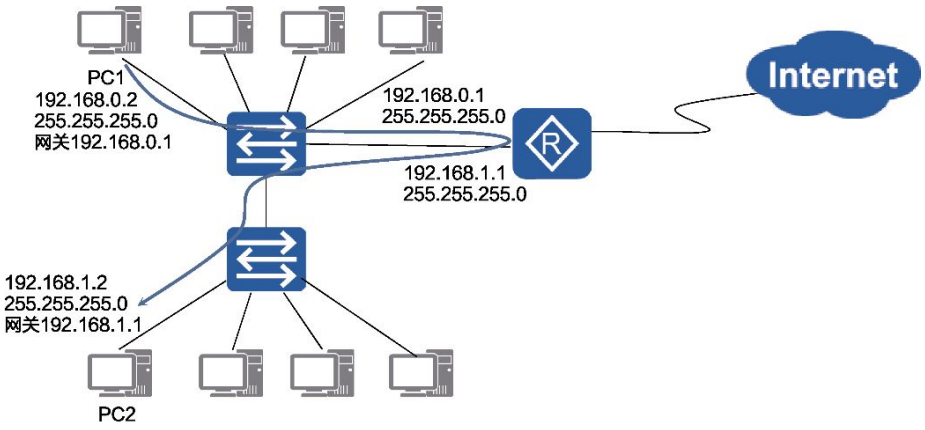


图3-44　两个网段的地址

有没有更好的办法，可以让这两个C类网段的计算机逻辑上在一个网段？这就需要将192.168.0.0/24和192.168.1.0/24这两个C类网络合并。

如图3-45所示，将这两个网段的IP地址的第3部分和第4部分写成二进制，可以看到将子网掩码往左移动1位（子网掩码中1的数量减少1），两个网段的网络部分就一样了，两个网段就在一个网段了。

	网络部分			主机部分
192.168.0.0	192	168	00000000	00000000
192.168.1.0	192	168	00000001	00000000
子网掩码	11111111	11111111	11111110	00000000
子网掩码	255	255	254	0

图3-45　合并两个子网

合并后的网段为192.168.0.0/23，子网掩码写成十进制为255.255.254.0，可用地址为192. 168.0.1～192.168.1.254。网络中计算机的IP地址和路由器接口的地址配置，如图3-46所示。

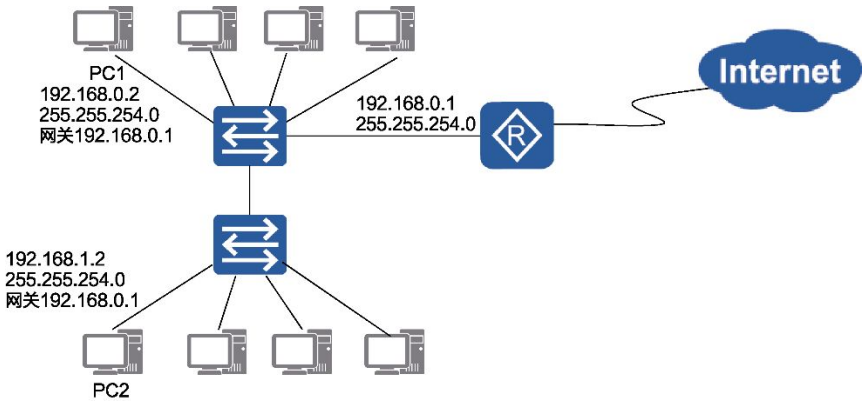


图3-46　合并后的地址配置

合并之后，IP地址192.168.0.255/23就可以给计算机使用。你也许觉得该地址的主机位全部是1，不能给计算机使用。但是把这个IP地址的第3部分和第4部分写成二进制就会看出主机位并不全为1，如图3-47所示。

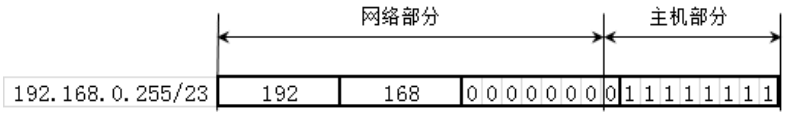


图3-47　确定是否是广播地址的方法

规律：子网掩码往左移1位，能够合并两个连续的网段，但不是任何连续的网段都能合并。下面讲解合并网段的规律。

3.6.2　合并网段的规律

前面讲了子网掩码往左移动1位，能够合并两个连续的网段，但不是任何两个连续的网段都能通过该方法合并成1个网段。

比如192.168.1.0/24和192.168.2.0/24就不能通过向左移动1位子网掩码来合并成一个网段。将这两个网段的第3部分和第4部分写成二进制能够看出来，如图3-48所示，向左移动1位子网掩码，这两个网段的网络部分还是不相同，说明不能合并成一个网段。



图3-48　合并网段的规律

子网掩码向左移动2位，其实就是合并了4个网段，如图3-49所示。

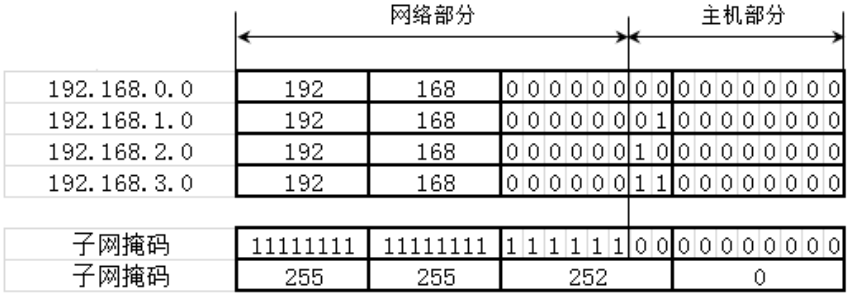


图3-49　合并网段的规律

下面讲解哪些连续的网段能够合并，即合并网段的规律。

（1）判断两个子网能否合并。

如图3-50所示，192.168.0.0/24和192.168.1.0/24子网掩码往左移1位，可以合并为一个网段192.168.0.0/23。



图3-50　合并192.168.0.0/24和192.168.1.0/24

如图3-51所示，192.168.2.0/24和192.168.3.0/24子网掩码往左移1位，可以合并为一个网段192.168.2.0/23。

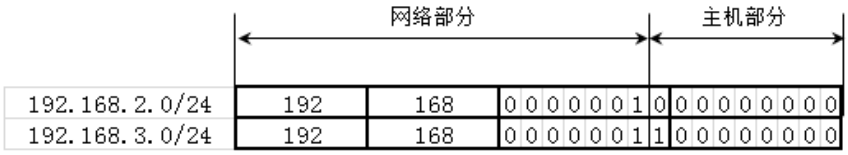


图3-51　合并192.168.2.0/24和192.168.3.0/24

可以看出规律，合并两个连续的网段，第一个网段的网络号写成二进制的最后一位是0，这两个网段就能合并。由3.1.2节所讲的规律，只要一个数能够被2整除，写成二进制最后一位肯定是0。

结论：判断连续的两个网段是否能够合并，只要第一个网络号能被2整除，就能够通过左移1位子网掩码合并成一个网段。

131.107.31.0/24和131.107.32.0/24是否能够左移1位子网掩码合并？

131.107.142.0/24和131.107.143.0/24是否能够左移1位子网掩码合并？

根据上面的结论：31除2，余1，131.107.31.0/24和131.107.32.0/24不能通过左移1位子网掩码合并成一个网段。

142除2，余0，131.107.142.0/24和131.107.143.0/24能通过左移1位子网掩码合并成一个网段。

（2）判断4个网段能否合并。

如图3-52所示，合并192.168.0.0/24、192.168.1.0/24、192.168.2.0/24和192.168.3.0/24 4个子网，子网掩码需要向左移动2位。

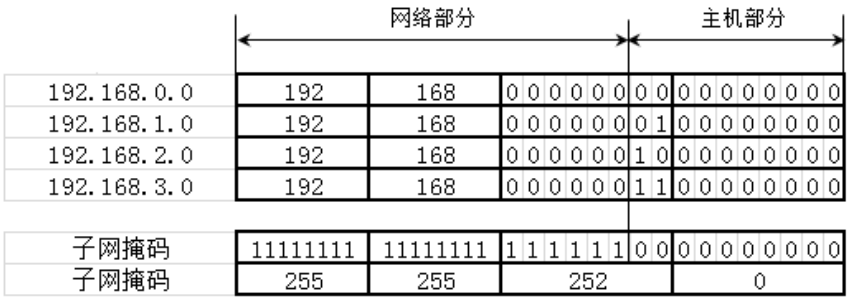


图3-52　合并4个网段

可以看到，合并192.168.4.0/24、192.168.5.0/24、192.168.6.0/24和192.168.7.0/24 4个子网，子网掩码需要向左移动2位，如图3-53所示。

规律：要合并连续的4个网络，只要第一个网段的网络号写成二进制后最后两位是00，这4个网段就能合并。根据3.1.2节讲到的二进制数的规律，只要一个数能够被4整除，写成二进制的最后两位肯定是00。



图3-53　合并4个网段

结论：判断连续的4个网段是否能够合并，只要第一个网段的网络号能被4整除，就能够通过左移2位子网掩码将这4个网段合并。

如图3-54所示，网段合并的规律如下：子网掩码左移1位能够合并2个网段，左移2位能够合并4个网段，左移3位能够合并8个网段。

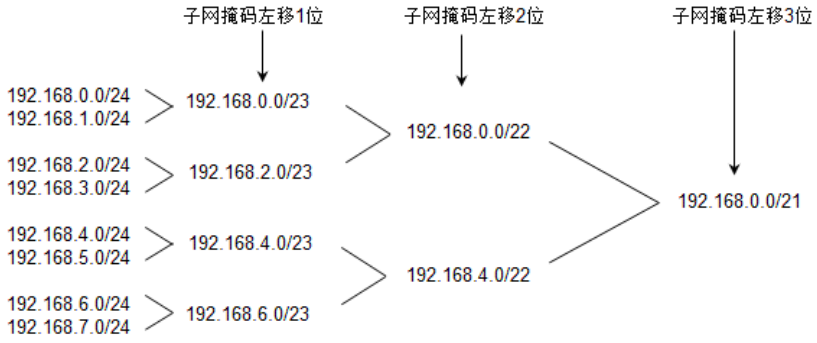


图3-54　网段合并的规律

规律：子网掩码左移n位，能合并的网段数量是2^n。

3.6.3　判断一个网段是超网还是子网

左移子网掩码可合并多个网段，右移子网掩码可将一个网段划分成多个子网，这使得IP地址打破了传统的A类、B类、C类网络的界限。

判断一个网段到底是子网还是超网，就要看该网段是A类网络、B类网络还是C类网络。默认A类地址的子网掩码是/8、B类地址的子网掩码是/16、C类地址的子网掩码是/24。如果该网段的子网掩码比默认子网掩码长（子网掩码1的个数多于默认子网掩码1的个数），就是子网；如果该网段的子网掩码比默认子网掩码短（子网掩码1的个数少于默认子网掩码1的个数），则是超网。

12.3.0.0/16是A类网络还是C类网络呢？是超网还是子网呢？该IP地址的第一部分是12，这是一个A类网络，A类地址的默认子网掩码是/8，该IP地址的子网掩码是/16，比默认子网掩码长，所以说这是A类网结的一个子网。

222.3.0.0/16是C类网络还是B类网络呢？是超网还是子网呢？该IP地址的第一部分是222，这是一个C类网络，C类地址的默认子网掩码是/24，该IP地址的子网掩码是/16，比默认子网掩码短，所示说这是一个合并了222.3.0.0/24～222.3.255.0/24共256个C类网络的超网。

3.7　习题

1．根据图3-55所示的网络拓扑和网络中的主机数量，将左侧的IP地址拖放到合适的接口。

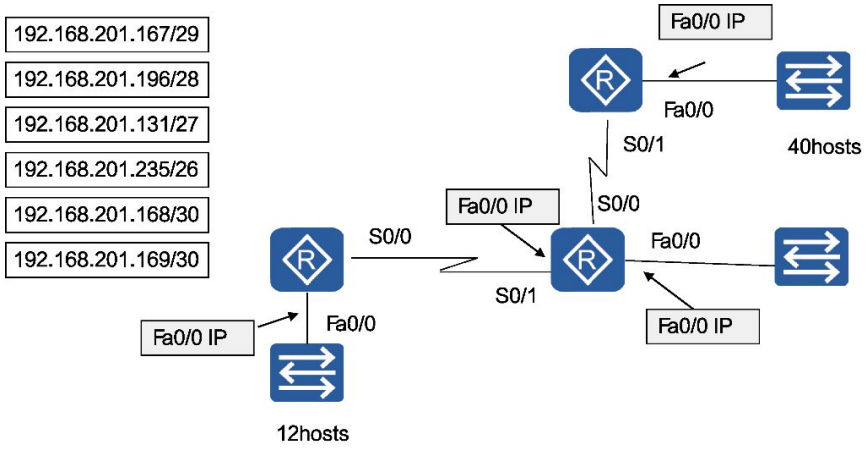


图3-55　网络规划

2．以下哪几个地址属于115.64.4.0/22网段？（　　）（选择3个答案）

A．115.64.8.32

B．115.64.7.64

C．115.64.6.255

D．115.64.3.255

E．115.64.5.128　　F．115.64.12.128

3．子网（　　）被包含在172.31.80.0/20网络。（选择2个答案）

A．172.31.17.4/30

B．172.31.51.16/30

C．172.31.64.0/18

D．172.31.80.0/22

E．172.31.92.0/22　　F．172.31.192.0/18

4．某公司设计网络，需要300个子网，每个子网的主机数量最大为50，对一个B类网络进行子网划分，下面的子网掩码（　　）可以采用。（选择2个答案）

A．255.255.255.0

B．255.255.255.128

C．255.255.255.224

D．255.255.255.192

5．网段172.25.0.0/16被分成8个等长子网，下面的地址（　　）属于第三个子网。（选择3个答案）

A．172.25.78.243

B. 172.25.98.16

C. 172.25.72.0

D. 172.25.94.255

E. 172.25.96.17　　F. 172.25.100.16

6. 根据图3-56，以下网段（　　）能够指派给网络A和链路A。（选择2个答案）

A. 网络A——172.16.3.48/26

B. 网络A——172.16.3.128/25

C. 网络A——172.16.3.192/26

D. 链路A——172.16.3.0/30

E. 链路A——172.16.3.40/30　　F. 链路A——172.16.3.112/30

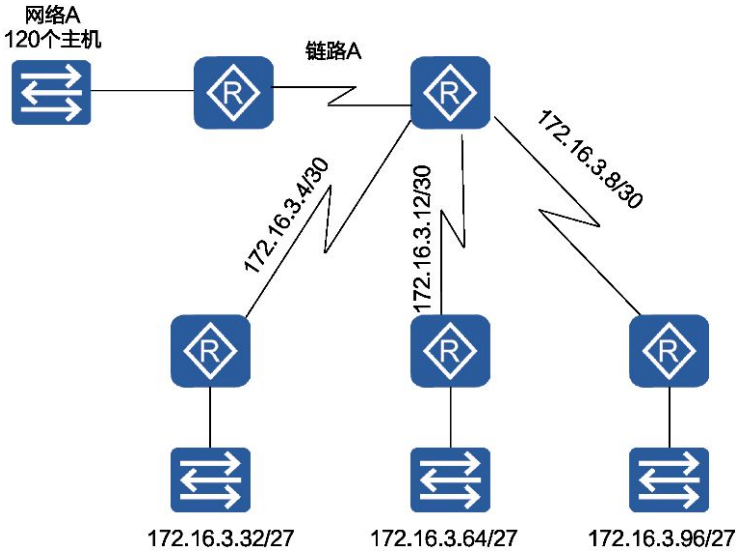


图3-56　网络拓扑

7．以下属于私网地址的是（　　）。

A．192.178.32.0/24

B．128.168.32.0/24

C．172.15.32.0/24

D．192.168.32.0/24

8．网络122.21.136.0/22中可用的最大地址数量是（　　）。

A．102

B．1023

C．1022

D. 1000

9. 主机地址192.15.2.160所在的网络是（　　）。

A. 192.15.2.64/26

B. 192.15.2.128/26

C. 192.15.2.96/26

D. 192.15.2.192/26

10. 某公司的网络地址为192.168.1.0/24，要划分成5个子网，每个子网最多20台主机，则适用的子网掩码是（　　）。

A. 255.255.255.192

B. 255.255.255.240

C. 255.255.255.224

D. 255.255.255.248

11. 某端口的IP地址为202.16.7.131/26，该IP地址所在网络的广播地址是（　　）。

A. 202.16.7.255

B. 202.16.7.129

C. 202.16.7.191

D. 202.16.7.252

12. 在IPv4中，组播地址是（　　）地址。

A. A类

B. B类

C. C类

D. D类

13. 某主机的IP地址为180.80.77.55、子网掩码为255.255.252.0，该主机向所在的子网发送广播分组，则目的地址可以是（　　）。

A. 180.80.76.0

B. 180.80.76.255

C. 180.80.77.255

D. 180.80.79.255

14. 某网络的IP地址空间为192.168.5.0/24，采用等长子网划分，子网掩码为255.255.255.248，则划分的子网个数为（　　），每个子网中的最大可分配地址数量为（　　）。

A. 32，6

B. 32，8

C. 8，32

D. 8，30

15. 网络管理员希望能够有效利用192.168.176.0/25网段的IP地址，现公司市场部门有20台主机，则最好分配下面哪个网段给市场部？（　　）

A. 192.168.176.0/25

B. 192.168.176.160/27

C. 192.168.176.48/29

D. 192.168.176.96/27

16. 一台Windows主机初次启动，如果无法从DHCP服务器获取IP地址，那么此主机可能会使用下列哪个IP地址？（　　）

A. 0.0.0.0

B. 127.0.0.1

C. 169.254.2.33

D. 255.255.255.255

17. 对于地址192.168.19.255/20，下列说法中正确的是（　　）。

A. 这是一个广播地址

B. 这是一个网络地址q+RS3S Ai0

C. 这是一个私有地址

D. 该地址在192.168.19.0网段上

18. 将192.168.10.0/24网段划分成3个子网，每个子网的计算机数量如图3-57所示，写出各个网段的子网掩码和能够分配给计算机使用的第一个可用地址和最后一个可用地址。

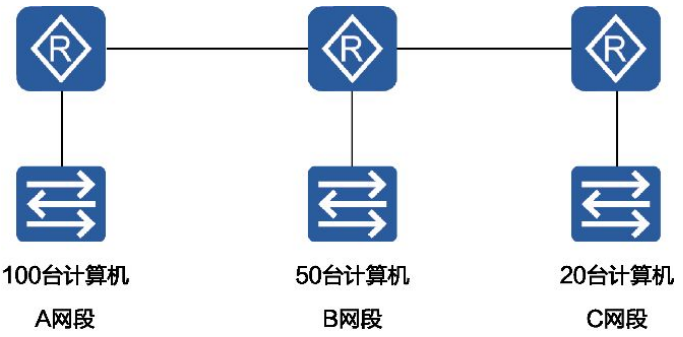


图3-57　子网划分示意图

第一个可用地址　　最后一个可用地址　　子网掩码

A网

段 _____ _____ _____

B网

段 _____ _____ _____

C网

段 _____ _____ _____

第4章　管理华为设备

本章内容

- 介绍华为网络设备操作系统
- eNSP简介
- 路由器的基本操作
- 配置文件的管理
- 捕获数据包

配置华为的路由器、交换机以及防火墙等网络设备就要熟悉其操作系统。华为公司为这些网络设备开发了通用的操作系统，通用路由平台（Versatile Routing Platform，VRP）就是华为公司为网络设备准备的通用网络操作系统。

在本章，你将配置eNSP中的网络设备，以实现和物理机的通信。

VRP为用户提供了命令行界面（Command-Line Interface，CLI），管理网络设备需要用户掌握命令行的使用方法。

第一次配置华为网络设备时通常通过Console口登录。配置好网络后，就可以通过telnet、SSH、Web登录网络设备以进行设备配置操作。网络设备的常规配置包括更改设备名称、设置设备时钟、给网络设备接口配置IP地址以及设置登录密码等。

设备配置完成后会立即生效，此时可输入display current-configuration命令来查看当前生效的配置；输入display saved-configuration命令来保存当前配置，也可以更改下一次启动加载的配置文件。

VRP通过文件系统来对设备上的所有文件（包括设备的配置文件、系统文件、License文件、补丁文件）和目录进行管理。VRP文件系统主要用来创建、删除、修改、复制和显示文件及目录。管理存储中的文件，设置启动配置文件，将这些配置文件通过TFTP和FTP导出以实现备份。

4.1　介绍华为网络设备操作系统

通用路由平台（Versatile Routing Platform，VRP）是华为公司数据通信产品的通用网络操作系统。目前，在全球各地的网络通信系统中，华为设备几乎无处不在，因此，学习、了解VRP的相关知识对于网络通信技术人员来说就显得尤为重要。

VRP是华为公司具有完全自主知识产权的网络操作系统，可以运行在从低端到高端的全系列路由器、交换机等数据通信产品的通用网络操作系统中，如同微软公司的Windows操作系统，苹果公司的iOS操作系统。VRP可以运行在多种硬件平台之上，如图4-1所示，包括路由器、局域网交换机、ATM交换机、拨号访问服务器、IP电话网关、电信级综合业务接入平台、智能业务选择网关，以及专用硬件防火墙等。VRP拥有一致的网络界面、用户界面和管理界面，为用户提供了灵活丰富的应用解决方案。



图4-1　运行VRP平台的设备

VRP平台以TCP/IP簇为核心，实现了数据链路层、网络层和应用层的多种协议，在操作系统中集成了路由交换技术、QoS技术、安全技术和IP语音技术等功能，并以IP转发引擎技术作为基础，为网络设备提供了出色的数据转发能力。

4.2 eNSP简介

eNSP（Enterprise Network Simulation Platform）是由华为提供的一款免费、可扩展、图形化操作的网络仿真工具平台，主要用于对企业网络路由器、交换机等设备进行软件仿真，可完美呈现真实设备实景，支持大型网络模拟，让广大用户有机会在没有真实设备的情况下进行模拟演练，学习网络技术。

eNSP最大的特点是高度仿真，其他特点具体如下。

- 可模拟华为AR路由器、x7系列交换机的大部分特性。
- 可模拟PC终端、Hub、云、帧中继交换机。
- 具备仿真设备配置功能，可快速学习华为命令行。
- 可模拟大规模网络。
- 可通过网卡实现与真实网络设备间的通信。
- 可以抓取任意链路中的数据包，直观展示协议交互过程。

4.2.1 安装eNSP

eNSP需要Virtual Box来运行路由器和交换机操作系统，使用Wireshark捕获链路中的数据包。当前华为官网提供的eNSP安装包中包含这两款软件，当然这两款软件也可以单独下载安装，先安装Virtual Box和Wireshark，最后安装eNSP。

下面的操作在Windows 10企业版（X64）上进行，先安装VirtualBox-5.2.6-120294-Win. exe，再安装Wireshark-win64-

2.4.4.exe，最后安装eNSP V100R002C00B510 Setup.exe。

安装eNSP时，出现图4-2所示的eNSP安装界面，不要选择“安装WinPcap4.1.3”“安装Wireshark”和“安装VirtualBox5.1.24”，因为这些都已经提前安装好了。

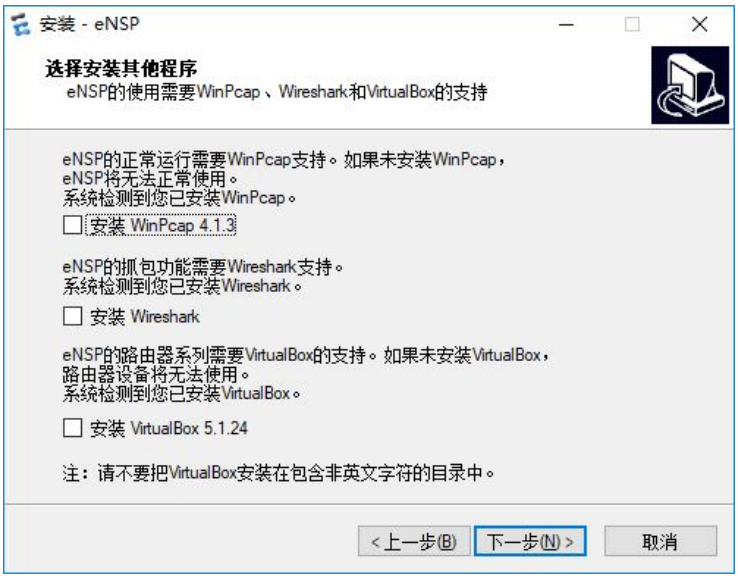


图4-2　eNSP安装界面

4.2.2　华为设备型号

华为交换机和路由设备有不同的型号，下面讲解华为设备的命名规则。

S系列是以太网交换机。从交换机的主要应用环境或用户定位来划分，企业园区网接入层主要应用的是S2700和S3700两大系列，汇聚层主要应用的是S5700系列，核心层主要应用的是S7700、S9300和S9700系列。同一系列交换机版本分为精简版（LI）、标准版（SI）、增强

版（EI）、高级版（HI）。如：S2700-26TP-PWR-EI表示VRP设备软件版本类型为增强版。

AR系列是访问路由器。路由器型号前面的AR是 Access Router（访问路由器）单词的首字母组合。AR系列的企业路由器有多个型号，包括AR150、AR200、AR1200、AR2200、AR3200。它们是华为第三代路由器产品，提供路由、交换、无线、语音和安全等功能。AR路由器被部署在企业网络和公网之间，作为两个网络间传输数据的入口和出口。在AR路由器上部署多种业务能降低企业的网络建设成本和运维成本。根据一个企业的用户数和业务的复杂程度可以选择将不同型号的AR路由器部署到网络中。

下面就以AR201路由器为例，可以看到该型号路由的接口（见图4-3）和支持的模块。 可以看到有CON/AUX端口，一个WAN口和8个FE（FastEthernet，快速以太网接口，100M口）接口。

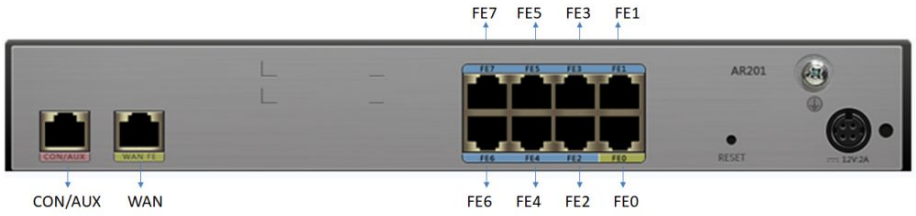


图4-3　AR201路由器接口

AR201路由器是面向小企业网络的设备，相当于一台路由器和一台交换机的组合。8个FE端口是交换机端口，WAN端口就是路由器端口（路由器端口连接不同的网段，可以设置IP地址作为计算机的网关；交换机端口连接计算机，不能配置IP地址）。路由器使用逻辑接口

Vlanif 1和交换机连接，交换机的所有端口默认都属于VLAN1，AR201路由器逻辑结构如图4-4所示。

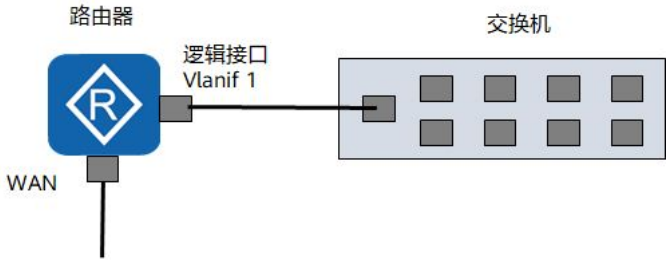


图4-4　AR201路由器等价的逻辑结构

以AR1220系列路由器为例说明模块化路由器的接口类型。AR1220是面向中型企业总部或大中型企业分支，以宽带、专线接入、语音和安全场景为主的多业务路由器。该型号的路由器是模块化路由器，有两个插槽可以根据需要插入合适的模块，有两个吉比特以太网接口，分别是GE0和GE1，这两个接口是路由器接口，8个FE接口是交换机接口。该设备也相当于两个设备——路由器和交换机，如图4-5所示。

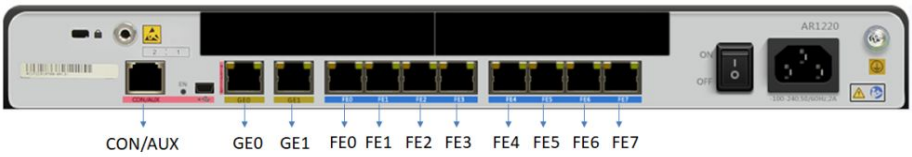


图4-5　AR1220路由器

接下来介绍端口命名规则，以4GEW-T为例。

- 4：表示4个端口。
- GE：表示千兆以太网。
- W：表示WAN接口板，这里的WAN表示三层接口。
- T：表示电接口。

端口命中还有以下标识。

- FE：表示快速以太网接口。
- L2：表示2层接口，即交换机接口。
- L3：表示3层接口，即路由器接口。
- POS：表示光纤接口。

图4-6列出了常见的接口图片和接口描述。

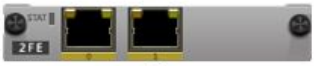
接口	描述
 1GEC	1 端口-GE COMBO WAN 接口卡
 2FE	2 端口-FE WAN 接口卡
 4GEW-T	4 端口-GE 电口 WAN 接口卡
 8FE1GE	9 端口-8FE/1GE L2/L3 以太接口卡
 24GE	24 端口-GE L2/L3 以太接口卡
 2SA	2 端口-同异步WAN 接口卡
 1POS	1 端口-POS 光口 接口卡
 2E1-F	2 端口-非通道化E1/T1 WAN 接口卡
 4G.SHDSL	4 线对G.SHDSL WAN 接口卡

图4-6　接口和描述

4.3 VRP命令行

4.3.1 命令行的基本概念

1. 命令行

华为网络设备功能的配置和业务的部署是通过VRP命令行来完成的。命令行是在设备内部注册的、具有一定格式和功能的字符串。一条命令行由关键字和参数组成，关键字是一组与命令行功能相关的单词或词组，通过关键字可以唯一确定一条命令行。参数是为了完善命令行的格式或指示命令的作用对象而指定的相关单词或数字等，包括整数、字符串、枚举值等数据类型，本书正文中采用斜体字体方式来标识命令行的参数。例如，测试设备间连通性的命令行ping *ip-address*中，ping为命令行的关键字，*ip-address*为参数（取值为一个IP地址）。

新购买的华为网络设备的初始配置为空。若希望它能够具有诸如文件传输、网络互通等功能，则需要首先进入到该设备的命令行界面，并使用相应的命令进行配置。

2. 命令行界面

命令行界面是用户与设备之间的文本类指令交互的界面，就如同Windows操作系统中的DOS（Disk Operation System）窗口一样。VRP

命令行界面如图4-7所示。

VRP命令的总数达上千条之多，为了实现对它们的分级管理，VRP系统将这些命令按照功能类型的不同分别注册在了不同的视图之下。

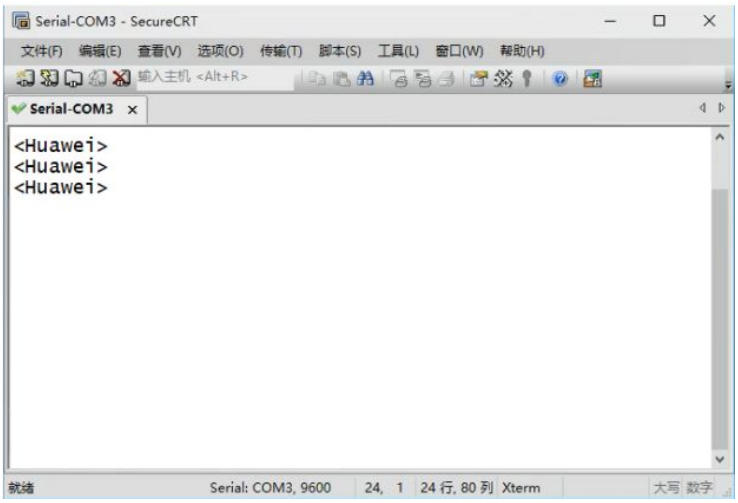


图4-7　VRP命令行界面

3. 命令行视图

命令行界面分成了若干种命令行视图，使用某个命令行时，需要先进入到该命令行所在的视图。最常用的命令行视图有用户视图、系统视图和接口视图，三者之间既有联系，又有一定的区别。

如图 4-8 所示，华为设备登录后，先进入用户视图<R1>，提示符”<R1>”中，“<>”表示用户视图，“R1”是设备的主机名。在用户视图下，用户可以了解设备的基础信息、查询设备状态，但不能进行与业务功能相关的配置。如果需要对设备进行业务功能配置，则需要进入到系统视图。

输入system-view进入系统视图[R1]，此时你可以配置系统参数。提示符“[R1]”中使用了方括号“[ ]”。系统视图下可以使用绝大部分的基础功能配置命令，在系统视图下可以配置路由器的一些全局参数，比如路由器主机名称等。

在系统视图下可以进入接口视图、协议视图、AAA视图等。配置接口参数、配置路由协议参数、配置IP地址池参数等都要进入相应的视图。进入不同的视图，就能使用该视图下的命令。若希望进入其他视图，必须先进入系统视图。

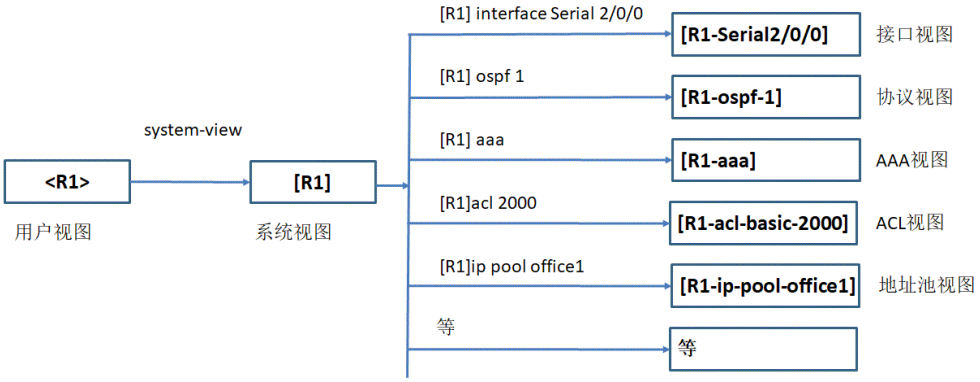


图4-8　视图

- 输入quit命令可以返回上一级视图。
- 输入return直接返回用户视图。
- 按快捷键<Ctrl+Z>可以返回用户视图。

进入不同的视图，提示内容会有相应变化，比如，进入接口视图后，主机名后会追加接口类型和接口编号的信息。在接口视图中，用户可以完成对相应接口的配置操作，例如配置接口的IP地址等。

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 192.168.10.111 24
```

VRP系统将命令和用户进行了分级，每条命令都有相应的级别，每个用户也都有自己的权限级别，并且用户权限级别与命令级别具有一定的对应关系。具有一定权限级别的用户登录以后，只能执行等于或低于自己级别的命令。

4. 命令级别与用户权限级别

VRP命令级别分为0～3级：0级（参观级）、1级（监控级）、2级（配置级）、3级（管理级）。网络诊断类命令属于参观级命令，用于测试网络是否连通等。监控级命令用于查看网络状态和设备基本信息。对设备进行业务配置时，需要用到配置级命令。对于一些特殊的功能，如上传或下载配置文件，则需要用到管理级命令。

用户权限分为0～15共16个级别。默认情况下，3级用户就可以操作VRP系统的所有命令，也就是说4～15级的用户权限在默认情况下与3级用户的权限一致的。4～15级的用户权限一般与提升命令级别的功能一起使用，例如当设备管理员较多时，需要在管理员中再进行权限细分，这时可以将某条关键命令所对应的用户级别提高，如提高到15级，这样一来，默认的3级管理员便不能再使用该关键命令了。

命令级别与用户权限级别的对应关系如表4-1所示。

表4-1　对应关系

用户级别	命令级别	说　　明
0	0	网络诊断类命令（ping、tracert）、从本设备访问其他设备的命令（telnet）等
1	0、1	系统维护命令，包括display等。但并不是所有的display命令都是监控级的，例如display current-configuration和display saved- configuration都是管理级命令
2	0、1、2	业务配置命令，包括路由、各个网络层次的命令等
3～15	0、1、2、3	涉及系统基本运行的命令，如文件系统、FTP下载、配置文件切换命令、用户管理命令、命令级别设置命令、系统内部参数设置命令等，还包括故障诊断的debugging命令

4.3.2　命令行的使用方法

1．进入命令视图

用户进入VRP系统后，首先进入的就是用户视图。如果出现<Huawei>，并有光标在“>”右边闪动，则表明用户已成功进入了用户视图。

```
<Huawei>
```

进入用户视图后，用便可以通过命令来了解设备的基础信息、查询设备状态等。如果需要对GigabitEthernet1/0/0接口进行配置，则需先使用system-view命令进入系统视图，再使用interface *interface-type interface-number*命令进入相应的接口视图。

```
<Huawei>system-view                                  -- 进入系统视图
[Huawei]
[Huawei]interface gigabitethernet 1/0/0      --进入接口视图
[Huawei-GigabitEthernet1/0/0]
```

2. 退出命令视图

quit命令的功能是从任何一个视图退出到上一层视图。例如，接口视图是从系统视图进入的，所以系统视图是接口视图的上一层视图。

```
[Huawei-GigabitEthernet1/0/0] quit           --退出到系统视图
[Huawei]
```

如果希望继续退出至用户视图，可再次执行quit命令。

```
[Huawei]quit                                         --退出到用户视图
<Huawei>
```

有些命令视图的层级很深，从当前视图退出到用户视图，需要多次执行quit命令。使用return命令，可以直接从当前视图退出到用户视图。

```
[Huawei-GigabitEthernetI/0/0]return          --退出到用户视图
<Huawei>
```

另外，在任意视图下，使用快捷键<Ctrl+Z>，可以达到与使用return命令相同的效果。

3. 输入命令行

VRP系统提供了丰富的命令行输入方法，支持多行输入，每条命令的最大长度为510个字符，命令关键字不区分大小写，同时支持不完整关键字输入。表4-2列出了命令行输入过程中常用的一些功能键。

表4-2　常用的功能键

功　能　键	功　　能
退格键 BackSpace	删除光标位置的前一个字符，光标左移，若已经到达命令起始位置，则停止
左光标键←或 快捷键 <Ctrl+B>	光标向左移动一个字符位置，若已经到达命令起始位置，则停止
右光标键→或 快捷键 <Ctrl+F>	光标向右移动一个字符位置：若已经到达命令尾部，则停止

功　能　键	功　　能
删除键Delete	删除光标所在位置的一个字符，光标位置保持不动，光标后方字符向左移动一个字符位置：若已经到达命令尾部，则停止
上光标键↑或快捷键<Ctrl+P>	显示上一条历史命令。如果需显示更早的历史命令，可以重复使用该功能键
下光标键↓或快捷键<Ctrl+N>	显示下一条历史命令，可重复使用该功能键

4. 不完整关键字输入

为了提高命令行输入的效率和准确性，VRP系统能够支持不完整的关键字输入功能，即在当前视图下，当输入的字符能够匹配唯一的关键字时，可以不必输入完整的关键字。例如，当需要输入命令display current-configuration时，可以通过输入d cu、di cu或discu来实现，但不能输入d c或dis c等，因为系统内有多条以d c、dis c开头的命令，如：display cpu-defend、display clock和display current-configuration。

5. 在线帮助

在线帮助是VRP系统提供的一种实时帮助功能。在命令行输入过程中，用户可以随时键入“？”以获得在线帮助信息。命令行在线帮助可分为完全帮助和部分帮助。

关于完全帮助，我们来看一个例子。假如我们希望查看设备的当前配置情况，但在进入用户视图后不知道下一步该如何操作，这时就可以键入“？”，得到如下的回显帮助信息。

```
<Huawei>?
User view commands:
  arp-ping                  ARP-ping
  autosave                  <Group> autosave command group
  backup                    Backup  information
 ……
  dialer                    Dialer
  dir                       List files on a filesystem
  display                   Display information
  factory-configuration  Factory configuration
---- More ----
```

从显示的关键字中可以看到“display”，对此关键字的解释为Display information。我们自然会想到，要查看设备的当前配置情况，很可能会用到“display”这个关键字。于是，按任意字母键退出帮助后，键入display和空格，再键入问号“？”，得到如下的回显帮助信息。

```
<Huawei>display ?
  Cellular                  Cellular interface
  aaa                       AAA
  access-user               User access
  accounting-scheme         Accounting scheme
……
  cpu-usage                 Cpu usage information
  current-configuration Current configuration
  cwmp                       CPE WAN Management Protocol
---- More ----
```

从回显信息中，我们发现了“current-configuration”。通过简单的分析和推理，我们便知道，要查看设备的当前配置情况，应该输入的命令行是“displaycurrent-configuration”。

再来看一个部分帮助的例子。通常情况下，我们不会完全不知道需要输入的命令行，会知道命令行关键字的部分字母。假如我们希望输入display current-configuration命令，但不记得完整的命令格式，只是记得关键字display的开头字母为dis，current-configuration的开头字母为c。此时，我们就可以利用部分帮助功能来确定出完整的命令。键入dis后，再键入问号“？”。

```
<Huawei>dis?
display Display information
```

回显信息表明，以dis开头的关键字只有display。根据不完整关键字输入原则，用dis就可以唯一确定关键字display。所以，在输入dis后直接输入空格，然后输入c，最后输入“？”，以获取下一个关键字的帮助。

```
<Huawei>dis c?
  <0-0>                    Slot number
  Cellular                 Cellular interface
  calibrate                Global calibrate
  capwap                   CAPWAP
  channel                  Informational channel status and
configuration
                           information
  clock                    Clock status and configuration
information
  config                   System config
  controller               Specify controller
  cpos                     CPOS controller
  cpu-defend               Configure CPU defend policy
  cpu-usage                Cpu usage information
```

```
current-configuration  Current configuration
cwmp                       CPE WAN Management Protocol
```

回显信息表明，关键字display后，以c开头的关键只有为数不多的十几个，从中很容易找到current-configuration。至此，我们便从dis和c这样的记忆片段中恢复出了完整的命令行display current-configuration。

6. 快捷键

快捷键的使用可以进一步提高命令行的输入效率。VRP系统已经定义了一些快捷键，称为系统快捷键。系统快捷键的功能固定，用户不能再重新定义。常见的系统快捷键如表4-3所示。

表4-3　常见VRP系统快捷键

快　捷　键	功　　能
Ctrl+A	将光标移动到当前行的开始
Ctrl+E	将光标移动到当前行的末尾
ESC+N	将光标向下移动一行
ESC+P	将光标向上移动一行

快 捷 键	功 能
Ctrl+C	停止当前正在执行的功能
Ctrl+Z	返回到用户视图，功能相当于return命令
<Tab>键	部分帮助的功能，输入不完整的关键字后按下<Tab>键，系统自动补全关键字

VRP系统还允许用户自定义一些快捷键，但自定义快捷键可能会与某些操作命令发生混淆，所以一般情况下最好不要自定义快捷键。

4.4 登录设备

配置华为网络设备，可以使用Console口、telnet或SSH方式。本节介绍用户界面配置和登录设备的各种方式。

4.4.1 用户界面配置

1. 用户界面的概念

在与设备进行信息交互的过程中，不同的用户拥有不同的用户界面。使用Console口登录设备的用户，其用户界面对应了设备的物理Console接口；使用Telnet登录设备的用户，其用户界面对应了设备的虚拟接口（Virtual Type Terminal，VTY）。不同的设备支持的VTY总数可能不同。

如果希望对不同的用户进行登录控制，则需要首先进入到对应的用户界面视图进行相应的配置（如，规定用户权限级别、设置用户名和密码等）。例如，假设规定通过Console 口登录的用户的权限级别为3级，则相应的操作如下。

```
<Huawei>system-view
[Huawe]user-interface console 0                  --进入Console口用户的用户界面视图
[Huawei-ui-console0]user privilege level 3       --设置Console登录用户的权限级别为3
```

如果有多个用户登录设备，且每个用户都会有自己的用户界面，那么设备如何识别这些不同的用户界面呢？

2. 用户界面的编号

用户登录设备时，系统会根据该用户的登录方式，自动分配一个当前空闲且编号最小的相应类型的用户界面给该用户。用户界面的编号包括以下两种。

（1）相对编号。

相对编号的形式是：用户界面类型+序号。一般地，一台设备只有1个Console口（插卡式设备可能有多个Console口，每个主控板提供1个Console口），VTY类型的用户界面一般有15个（默认情况下，开启了其中的5个）。所以，相对编号的具体形式如下。

- Console口的编号：CON 0。
- VTY的编号：第一个为VTY 0，第二个为VTY 1，以此类推。

（2）绝对编号。

绝对编号仅仅是一个数值，用来唯一标识一个用户界面。绝对编号与相对编号具有一一对应的关系：Console用户界面的相对编号为CON0，对应的绝对编号为0；VTY用户界面的相对编号为VTY0～VTY14，对应的绝对编号为129～143。

使用display user-interface命令可以查看设备当前支持的用户界面信息，操作如下。可以看到CON 0有一个用户连接，权限级别为15，有一个用户通过虚拟接口连接VTY 0，权限级别为2，Auth表示身份验证模式，P代表password（只需输入密码），A代表AAA验证（需要输入用户名和密码）。

```
<Huawei>display user-interface
  Idx  Type    Tx/Rx   Modem Privi ActualPrivi    Auth   Int
+ 0    CON 0   9600    -     15      15             P     -
+ 129  VTY 0           -     2       2              A     -
  130  VTY 1           -     2     -                A     -
  131  VTY 2           -     2     -                A     -
  132  VTY 3           -     0     -                P     -
  133  VTY 4           -     0     -                P     -
  145  VTY 16          -     0     -                P     -
  146  VTY 17          -     0     -                P     -
  147  VTY 18          -     0     -                P     -
  148  VTY 19          -     0     -                P     -
  149  VTY 20          -     0     -                P     -
  150  Web 0   9600    -     15    -                A     -
  151  Web 1   9600    -     15    -                A     -
  152  Web 2   9600    -     15    -                A     -
  153  Web 3   9600    -     15    -                A     -
  154  Web 4   9600    -     15    -                A     -
  155  XML 0   9600    -     0     -                A     -
  156  XML 1   9600    -     0     -                A     -
  157  XML 2   9600    -     0     -                A     -
UI(s) not in async mode -or- with no hardware support:
1-128
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
   Int : The physical location of UIs.
```

回显信息中，第一行Idx表示绝对编号，第二行Type为对应的相对编号。

3. 用户验证

每个用户登录设备时都会有一个用户界面与之对应。那么，如何做到只有合法用户才能登录设备呢？答案是通过用户验证机制。设备支持的验证方式有3种：Password验证、AAA验证和None验证。

（1）Password验证。只需输入密码，密码验证通过后，即可登录设备。默认情况下，设备使用的是Password验证方式。使用该方式时，如果没有配置密码，则无法登录设备。

（2）AAA验证。需要输入用户名和密码，只有输入正确的用户名和与其对应的密码时，才能登录设备。由于需要同时验证用户名和密码，所以AAA验证方式的安全性比Password验证方式高，并且该方式可以区分不同的用户，用户之间互不干扰。使用Telnet登录时，一般都采用AAA验证方式。

（3）None验证。不需要输入用户名和密码，可直接登录设备，即无须进行任何验证。安全起见，不推荐使用这种验证方式。

用户验证机制保证了用户登录的合法性。默认情况下，通过Telnet登录的用户，在登录后的权限级别是0级。

4. 用户权限级别

前面已经对用户权限级别的含义以及它与命令级别的对应关系进行了介绍。用户权限级别也称为用户级别，默认情况下，用户级别在3级及以上时，便可以操作设备的所有命令。用户的级别可以在对应用户界面视图下执行user privilege level *level*命令进行配置，其中*level*为指定的用户级别。

有了以上这些关于用户界面的相关知识后，我们接下来通过两个实例来说明Console和VTY用户界面的配置方法。

4.4.2 通过Console口登录设备

路由器初次配置时，需要使用Console通信电缆来连接路由器的Console口和计算机的COM口，不过现在的笔记本大多没有COM口了。如图4-9所示，可以使用COM口转USB接口线缆，从而接入计算机的USB接口。

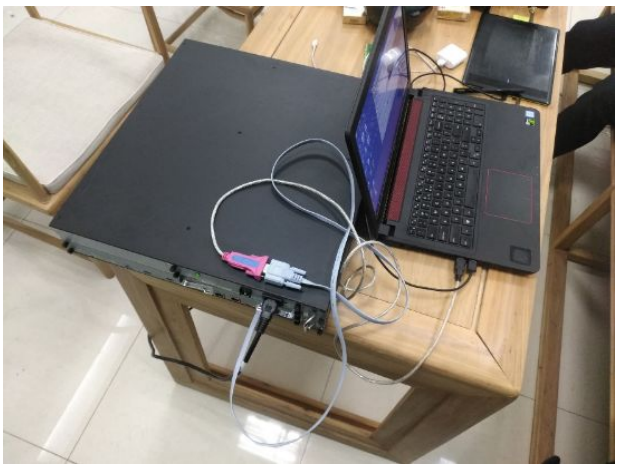


图4-9 Console配置路由器

如图4-10所示，在“计算机管理”界面，单击“设备管理器”。安装驱动后，可以看到USB接口充当了COM3接口。

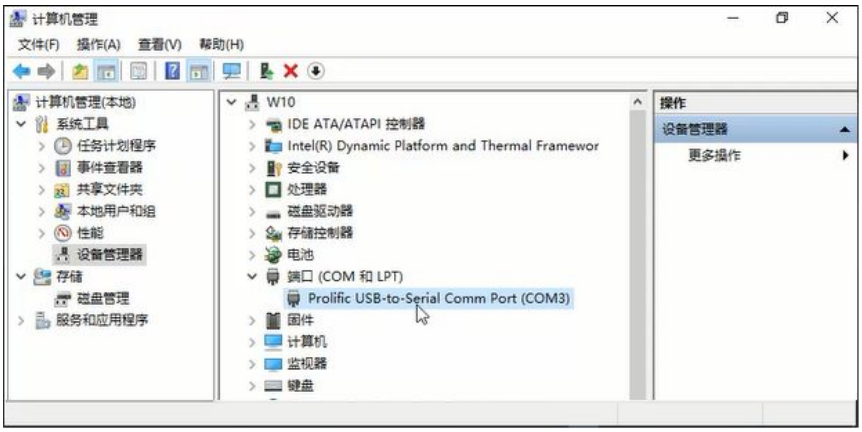


图4-10　查看USB接口充当的COM口

打开SecureCRT软件，如图4-11所示，在“SecureCRT协议”选项卡中选“Serial”，单击“下一步”。在出现的端口选择界面，如图4-12所示，在USB设备模拟出的“端口”选项卡中选择“COM3”。其他设置参照图4-12进行设置，然后单击“下一步”。

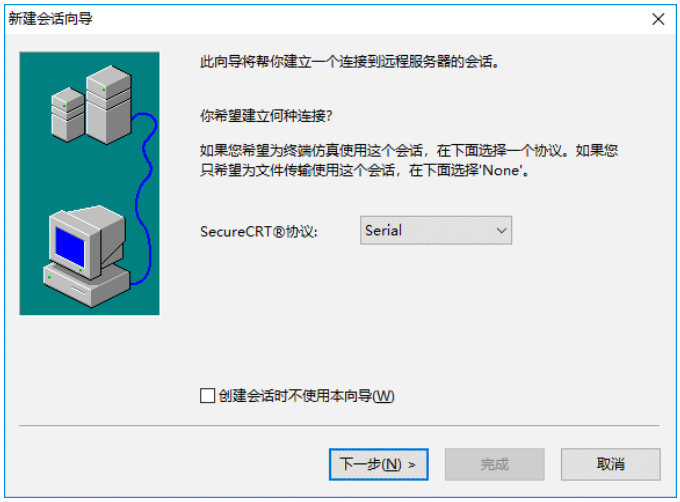


图4-11　选择协议

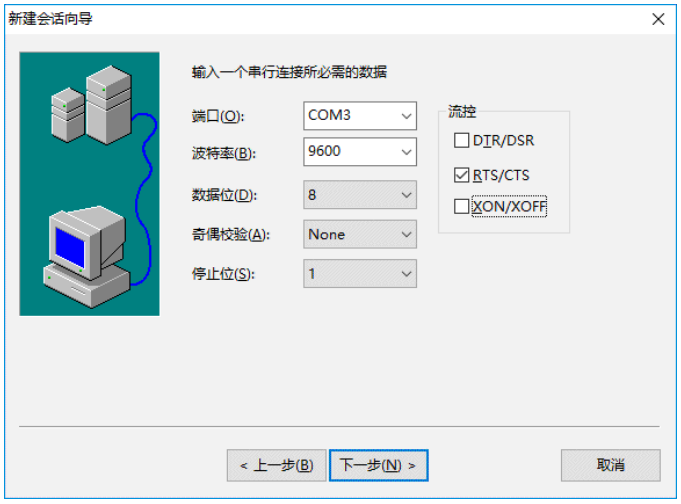


图4-12　选择端口、波特率等设置

Console用户界面对应从Console口直连登录的用户，一般采用Password验证方式。通过Console口登录的用户一般为网络管理员，需要最高级别的用户权限。

（1）进入Console用户界面。

进入Console用户界面使用的命令为user-interface console *interface-number*，*interface- number*表示console用户界面的相对编号，取值为0。

```
[Huawei]user-interface console 0
```

（2）配置用户界面。

在Console用户界面视图下配置验证方式为Password验证，并配置密码为91xueit，且密码将以密文形式保存在配置文件中。

配置用户界面的用户验证方式的命令为authentication-mode {aaa | password}。

```
[Huawei-ui-console0]authentication-mode ?
   aaa       AAA authentication
   password  Authentication through the password of a user
terminal interface
[Huawei-ui-console0]authentication-mode password
Please configure the login password (maximum length 16):91xueit
```

如果打算重设密码，可以输入以下命令，将密码设置为91xueit。

```
[Huawei-ui-console0]set authentication password cipher 91xueit
```

配置完成后，配置信息会保存在设备的内存中，使用命令display current-configuration即可进行查看。如果不进行存盘保存，则这些信息在设备通电或重启时将会丢失。

输入display current-configuration section user-interface命令会显示当前配置中user-interface的设置。如果只输入display current-configuration 会显示全部设置。

```
<Huawei>display current-configuration section user-interface
[V200R003C00]
#
user-interface con 0
 authentication-mode password
 set authentication password
cipher %$%${PA|GW3~G'2AJ%@K{;MA,$/:\,wmOC*yI7U_x!,wkv].$/=,%$%$
user-interface vty 0 4
user-interface vty 16 20
#
return
```

4.4.3 通过Telnet登录设备

VTY用户界面对应于使用Telnet方式登录的用户。考虑到Telnet是远程登录，存在安全隐患，所以在用户验证方式上采用了AAA验证。一般地，设备调试阶段需要登录设备的人员较多，并且需要进行业务方面的配置，所以通常将VTY用户界面数配置为最大——15，即允许最多15个用户同时使用Telnet方式登录到设备。同时，将用户级别设置为2级，即配置级，以便可以进行正常的业务配置。

（1）配置最大VTY用户界面数为15。

配置最大VTY用户界面数使用的命令是user-interface maximum-vty *number*。如果希望最大VTY用户界面数为15个，则*number*应取值为15。

```
[Huawei]user-interface maximum-vty 15
```

（2）进入VTY用户界面视图。

使用user-interface vty *first-ui-number* [*last-ui-number*]命令进入VTY用户界面视图，其中*first-ui-number*和*last-ui-number*为VTY用户界面的相对编号，方括号“[ ]”表示该参数为可选参数。假设现在需要对15个VTY用户界面进行整体配置，则*first-ui-number*应取值为0，*last-ui-number*取值为14。

```
[Huawei]user-interface vty 0 14
```

进入VTY用户界面视图：

```
[Huawei-ui-vty0-14]
```

（3）配置VTY用户界面的用户级别为2级。

配置用户级别的命令为user privilege level *level*。因为现在需要配置用户级别为2级，所以*level*的取值为2。

```
[Huawei-ui-vty0-14]user privilege level 2
```

（4）配置VTY用户界面的用户验证方式为AAA。

配置用户验证方式的命令为authentication-mode {aaa | password}，其中大括号“{ }”表示其中的参数应任选其一。

```
[Huawei-ui-vty0-14]authentication-mode aaa
```

（5）配置AAA验证方式的用户名和密码。

首先退出VTY用户界面视图，执行命令aaa，进入AAA视图。再执行命令local-user *user-name* password cipher *password*，配置用户名和密码。*user-name*表示用户名，*password*表示密码，关键字cipher表示配置的密码将以密文形式保存在配置文件中。最后，执行命令local-user *user-name* service-type telnet，定义这些用户的接入类型为Telnet。

```
[Huawei-ui-vty0-14]quit
[Huawei]aaa
[Huawei-aaa]local-user admin password cipher admin@123
[Huawei-aaa]local-user admin service-type telnet
[Huawei-aaa]quit
```

配置完成后，当用户通过Telnet方式登录设备时，设备会自动分配一个编号最小的可用VTY用户界面给用户使用，进入命令行界面之前需要输入上面配置的用户名（admin）和密码（admin@123）。

Telnet协议是TCP/IP协议族中应用层协议的一员。Telnet的工作方式为“服务器 / 客户端”方式，它提供了从一台设备（Telnet客户端）远程登录到另一台设备（Telnet服务器）的方法。Telnet服务器与Telnet客户端之间需要建立TCP连接，Telnet服务器的默认端口号为23。

VRP系统既支持Telnet服务器功能，也支持Telnet客户端功能。利用VRP系统，用户还可以先登录到某台设备，然后将这台设备作为Telnet客户端再通过Telnet方式远程登录到网络上的其他设备，从而可以更为灵活地实现对网络的维护操作。如图 4-13 所示，路由器R1既是PC的Telnet服务器，又是路由器的Telnet客户端。

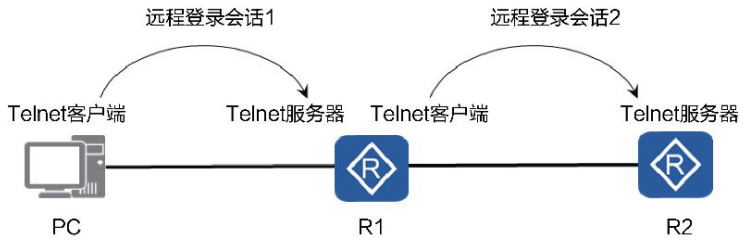


图4-13　Telnet二级连接

在Windows系统中，打开命令行工具，确保Windows系统和路由器的网络畅通。输入telnet *ip-address*后，再输入账户和密码，就能远程登录路由器进行配置。如图4-14所示，输入telnet 192.168.10.111

后输入账户和密码，登录<Huawei>成功。再输入telnet 172.16.1.2后输入密码，登录<R2>路由器成功。若想退出telnet，可输入quit。

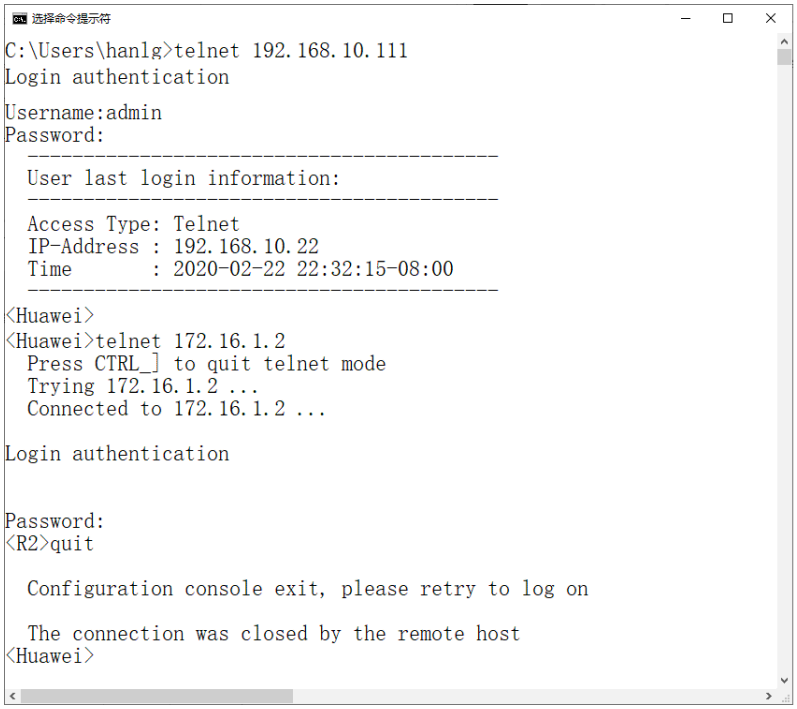


图4-14　在Windows上使用Telnet登录路由器

4.4.4　通过SSH登录设备

使用Telnet登录路由器，账号密码在网上是明文传输，不安全。通过网络登录路由器时使用SSH比telnet更安全。

SSH（Secure Shell）由IETF的网络小组（Network Working Group）所制定；SSH为建立在应用层基础上的安全协议。SSH是较可靠、专为远程登录会话和其他网络服务提供安全性的协议。利用SSH协议可以有效防止远程管理过程中的信息泄露问题。

从客户端来看，SSH提供两种级别的安全验证。

第一种级别是基于口令的安全验证。只要你知道自己的账号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证你正在连接的服务器就是你想连接的服务器。可能会有别的服务器冒充真正的服务器，也就是受到“中间人”方式的攻击。

第二种级别是基于密钥的安全验证。

该级别需要依靠密钥，也就是你必须为自己创建一对密钥，并把公用密钥放在需要访问的服务器上。如果你要连接到SSH服务器上，客户端软件就会向服务器发出请求，请求用你的密钥进行安全验证。服务器收到请求之后，先在该服务器上你的主目录中寻找你的公用密钥，然后把它和你发送过来的公用密钥进行比较。如果两个密钥一致，服务器就用公用密钥加密“质询”（challenge）并把它发送给客户端软件。客户端软件收到“质询”之后就可以用你的私人密钥解密再把它发送给服务器。

用这种方式，你必须知道自己密钥的口令。但是，与第一种级别相比，第二种级别不需要在网络上传送口令。

下面的操作将会把上面创建的admin用户的登录类型更改为SSH，设置SSH用户admin的认证模式是密码认证，开启路由器的SSH认证服务，生成本地认证密钥，并配置VTY使用SSH协议。

```
[Huawei-aaa]local-user admin service-type ?
   8021x      802.1x user
   bind       Bind authentication user
```

```
   ftp         FTP user
   http        Http user
   ppp         PPP user
   ssh         SSH user
   sslvpn      Sslvpn user
   telnet      Telnet  user
   terminal    Terminal user
   web         Web authentication user
   x25-pad     X25-pad user
[Huawei-aaa]local-user admin service-type ssh          --用户admin
认证默认是SSH
[Huawei-aaa]quit

[Huawei]ssh user admin authentication-type password    -- SSH用户
admin认证模式是密码认证
[Huawei]stelnet server enable                          --开启SSH认
证服务

[Huawei]rsa local-key-pair create                      -- 生成本地认
证密钥
The key name will be: Host
% RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
        It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
.........++++++++++++
.....++++++++++++
.........++++++++
.......++++++++

[Huawei]user-interface vty 0 14
[Huawei-ui-vty0-14]authentication-mode aaa      --设置虚拟终端认证模
式为AAA
[Huawei-ui-vty0-14]protocol inbound ssh         --开启SSH
[Huawei-ui-vty0-14]quit
```

在Windows上安装SecureCRT。SecureCRT是一款支持SSH（SSH1和SSH2）的终端仿真程序，简单地说是在Windows系统中登录UNIX、Linux服务器主机、华为网络设备的软件。打开SecureCRT，创建新的连接。如图4-15所示，选择连接使用的协议为SSH2，单击“下一

步”。如图4-16所示，输入路由器的地址、端口和登录账户，单击“下一步”。

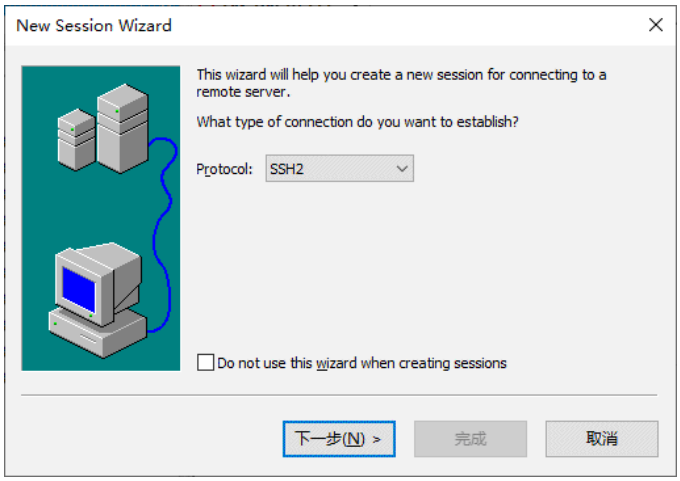


图4-15　选择协议

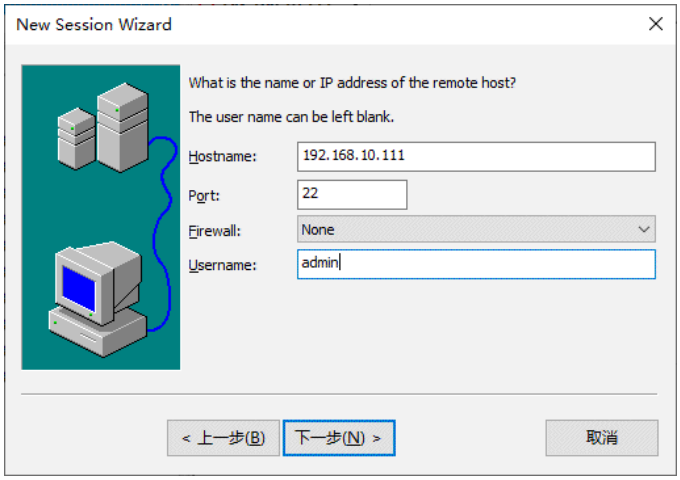


图4-16　输入路由器地址和登录账户

当单击创建的连接时，会出现一个对话框，如图4-17所示。输入登录账户的密码，单击“OK”。登录成功后进入用户视图，如图4-18所示。

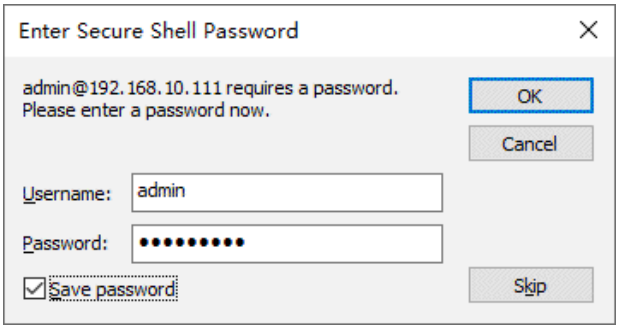


图4-17　输入账户的密码

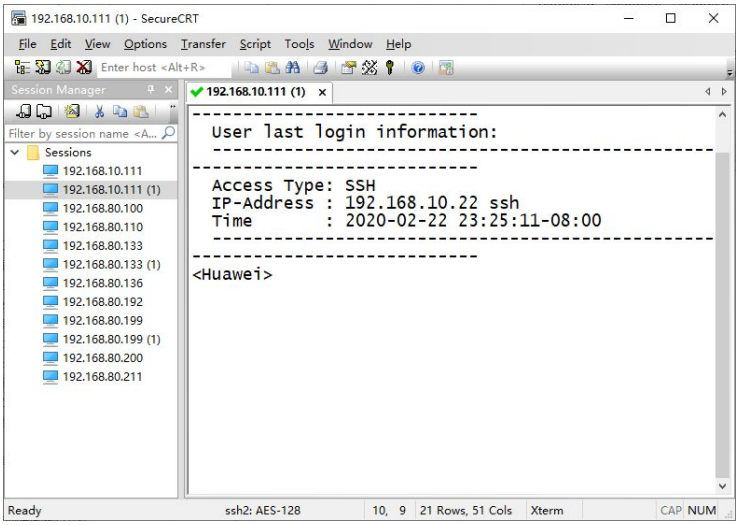


图4-18　用户视图

4.5 基本配置

下面讲述华为网络设备的一些基本配置，包括设置设备名称、更改系统时间、给接口设置IP地址，禁用启用接口等。

4.5.1 配置设备名称

命令行界面中的尖括号“< >”或方括号“[ ]”中包含设备的名称，它也称为设备主机名。默认情况下，设备名称为“Huawei”。为了更好地区分不同的设备，通常需要修改设备名称。我们可以通过命令加sysname *hostname*来对设备名称进行修改，其中sysname是命令行的关键字，*hostname*为参数，表示希望设置的设备名称。

例如，通过如下操作，就可以将设备名称设置为Huawei-AR-01。

```
<Huawei>?                                  --查看用户视图下可以执行的命令
<Huawei>system-view                        --进入系统视图
[Huawei]sysname Huawei-AR-01               --更改路由器名称为Huawei-AR-01
[Huawei-AR-01]
```

4.5.2 配置设备时钟

华为设备出厂时默认采用了协调世界时(UTC)，但没有配置时区，因此在配置设备系统时钟前，需要了解设备所在的时区。

设置时区的命令行为clock timezone *time-zone-name* { add | minus } *offset*，其中*time-zone- name*为用户定义的时区名，用于标

识配置的时区；根据偏移方向选择add和minus，正向偏移(UTC时间加上偏移量为当地时间）选择add，负向偏移(UTC时间减去偏移量为当地时间）选择minus；offset为偏移时间。假设设备位于北京时区，则相应的配置应该是（注意：设置时区和时间是在用户模式下）：

```
<Huawei>clock timezone BJ add 8:00
```

设置好时区后，就可以设置设备当前的日期和时间了。华为设备仅支持24小时制，使用的命令行为clock datetime *HH：MM：YYYY-MM-DD*，其中*HH：MM：SS*为设置的时间，*YYYY-MM-DD*为设置的日期。假设当前的日期为2020年2月23日，时间是16:37:00，则相应的配置应该是：

```
<Huawei>clock datetime 16:37:00 2020-02-23
```

输入display clock来显示当前设备的时区、日期和时间：

```
<Huawei>display clock
2020-02-23 16:37:07
Sunday
Time Zone(BJ) : UTC+08:00
```

4.5.3 配置设备IP地址

用户可以通过不同的方式登录到设备命令行界面，包括Console口登录和Telnet登录。首次登录新设备时，由于新设备为空配置设备，所以只能通过Console口或MiniUSB口登录。首次登录到新设备后，便可以给设备配置一个IP地址，然后开启Telnet功能。

IP地址是针对设备接口的配置，通常一个接口配置一个IP地址。配置接口IP地址的命令为ip address *ip-address* { *mask* | *mask-length* }，其中ip address是命令关键字，*ip-address*为希望配置的IP地址。*mask*表示点分十进制方式的子网掩码；*mask-length*表示子网掩码的长度，即子网掩码中二进制数1的个数。

假设设备Huawei的接口Ethernet 0/0/0，分配的IP地址为192.168.1.1，子网掩码为255. 255.255.0，则相应的配置应该是：

```
[Huawei]interface Ethernet 0/0/0     --进入接口视图
[Huawei-Ethernet0/0/0]ip address 192.168.1.1 255.255.255.0 --添加IP地址和子网掩码
[Huawei-Ethernet0/0/0]undo shutdown                          --启用接口
 [Huawei-Ethernet0/0/0]ip address 192.168.2.1 24 ?
  sub    Indicate a subordinate address
  <cr>   Please press ENTER to execute command
[Huawei-Ethernet0/0/0]ip address 192.168.2.1 24 sub          --给接口添加第二个地址
[Huawei-Ethernet0/0/0]display this                           --显示接口的配置
[V200R003C00]
#
interface Ethernet0/0/0
ip address 192.168.1.1 255.255.255.0
 ip address 192.168.2.1 255.255.255.0 sub
#
return
[Huawei-Ethernet0/0/0]quit                    --退出接口配置模式
```

输入display ip interface brief命令显示接口IP地址相关的摘要信息。

```
<Huawei>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
```

```
(s): spoofing
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 1

Interface                         IP Address/Mask      Physical
Protocol
Ethernet0/0/0                     192.168.1.1/24       up
up
Ethernet0/0/8                     unassigned           down
down
NULL0                             unassigned           up
up(s)
Vlanif1                           192.168.10.1/24      up
up
```

从以上输出可以看到，Ethernet0/0/0接口PHY（物理层）UP（启用），Protocol（数据链路层）也启用。

输入undo ip address删除接口配置的IP地址。

```
[Huawei-Ethernet0/0/0]undo ip address
```

4.6　配置文件的管理

华为设备配置更改后的设置会立即生效，成为当前配置，保存在内存中。如果设备断电重启或关机重启，则内存的配置会丢失；如果想让当前的配置在重启后依然生效，就需要将配置保存。下面就讲解华为网络设备中的配置文件，以及如何管理华为设备中的文件。

4.6.1　华为设备配置文件

本节介绍路由器的配置和配置文件。涉及3个概念：当前配置、配置文件和下次启动的配置文件。

1. 当前配置

设备内存中的配置就是当前配置，进入系统视图更改路由器的配置，就是更改当前配置。设备断电或重启时，内存中的所有信息（包括配置信息）全部消失。

2. 配置文件

包含设备配置信息的文件称为配置文件，它存在于设备的外部存储器中（注意，不是内存中），其文件名的格式一般为“*.cfg”或“*.zip”，用户可以将当前配置保存到配置文件中。设备重启时，配置文件的内容可以被重新加载到内存，成为新的当前配置。配置文件

除了可以保存配置信息，还可以方便维护人员查看、备份以及移植配置信息用于以其他设备。默认情况下，在保存当前配置时，设备会将配置信息保存到名为“vrpcfg.zip”的配置文件中，并将该文件保存到设备的外部存储器的根目录下。

3. 下次启动配置文件

保存配置时可以指定配置文件的名称，也就是保存的配置文件可以有多个。下次启动加载哪个配置文件，可以指定。默认情况下，下次启动的配置文件名为“vrpcfg.zip”。

4.6.2 保存当前配置

保存当前配置的方式有两种：手动保存和自动保存。

1. 手动保存配置

用户可以使用save［ *configuration-file* ］命令随时将当前配置以手动方式保存到配置文件中，参数*configuration-file*为指定的配置文件名，格式必须为“*.cfg”或“*.zip”。如果未指定配置文件名，则配置文件名默认为“vrpcfg.zip”。

例如，需要将当前配置保存到文件名为“vrpcfg.zip”的配置文件中时，可进行如下操作。

在用户视图中，使用save命令，再输入y以进行确认，从而保存路由器的配置。如果不指定保存配置的文件名，配置文件就是“vrpcfg.zip”。dir命令可以列出flash根目录下的全部文件和文件夹，这样就能看到这个配置文件。路由器中的flash相当于计算机中的硬盘，可以存放文件和保存的配置。

```
<R1>save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
--输入y
  It will take several minutes to save configuration file, please
wait.......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being
activated
```

如果还需要将当前配置保存到文件名为“backup.zip”的配置文件中，作为对vrpcfg.zip的备份，则可进行如下操作。

```
<Huawei>save backup.zip
 Are you sure to save the configuration to backup.zip? (y/n)[n]:y
  It will take several minutes to save configuration file, please
wait......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being
activated
```

2. 自动保存配置

自动保存配置功能可以有效降低用户因忘记保存配置而导致配置丢失的风险。自动保存功能分为周期性自动保存和定时自动保存两种方式。

在周期性自动保存方式下，设备会根据用户设定的保存周期，自动完成配置保存。无论设备的当前配置相比配置文件是否有变化，设备都会进行自动保存操作。在定时自动保存方式下，用户设定一个时间点，设备会每天在此时间点自动进行一次保存。默认情况下，设备的自动保存功能是关闭的，需要用户开启之后才能使用。

周期性自动保存的设置方法如下：首先执行命令autosave interval on，开启设备的周期性自动保存功能，然后执行命令autosave intervale *time*设置自动保存周期。*time*为指定的时间周期，单位为分钟，默认值为1440分钟（24小时）。

定时自动保存的设置方法如下：首先执行命令autosave time on，开启设备的定时自动保存功能，然后执行命令autosave time *time-value*，设置自动保存的时间点。*time-value*为指定的时间点，格式为hh:mm:ss。

以下命令打开周期性保存功能，设置自动保存间隔为120分钟。

```
<R1>autosave interval on                --打开周期性保存功能
  System autosave interval switch: on
  Autosave interval: 1440 minutes       --默认1440分钟保存一次
  Autosave type: configuration file
  System autosave modified configuration switch: on --如果配置更改为
30分钟自动保存
  Autosave interval: 30 minutes
  Autosave type: configuration file

<R1>autosave interval 120                --设置每隔120分钟自动保存
  System autosave interval switch: on
  Autosave interval: 120 minutes
  Autosave type: configuration file
```

周期性保存和定时保存不能同时启用。关闭周期性保存功能，再打开定时自动保存功能，更改定时保存时间为中午12点。

```
<R1>autosave interval off                    --关闭周期性保存功能
<R1>autosave time on                         --开启定时保存
  System autosave time switch: on
  Autosave time: 08:00:00                    --默认每天8点定时保存
  Autosave type: configuration file
<R1>autosave time ?                          --查看time后可以输入的参数
  ENUM<on,off>    Set the switch of saving configuration data
automatically by
                  absolute time
  TIME<hh:mm:ss>  Set the time for saving configuration data
automatically
<R1>autosave time 12:00:00                   --更改定时保存时间为12点
  System autosave time switch: on
  Autosave time: 12:00:00
  Autosave type: configuration file
```

默认情况下，设备会保存当前配置到“vrpcfg.zip”文件中。如果用户指定了另外一个配置文件作为设备下次启动的配置文件，则设备会将当前配置保存到新指定的下次启动的配置文件中。

4.6.3 设置下一次启动加载的配置文件

设备支持设置任何一个存在于设备的外部存储器的根目录下（如：flash:/）的“*.cfg”或“*.zip”文件作为设备的下次启动的配置文件。我们可以通过startup saved-configuration *configuration-file*命令来设置设备下次启动的配置文件，其中*configuration-file*为指定配置文件名。如果设备的外部存储器的根目录下没有该配置文件，则系统会提示设置失败。

例如，如果需要指定已经保存的backupzip文件作为下次启动的配置文件，可执行如下操作。

```
<R1>startup saved-configuration backup.zip                --指定下一次启动
加载的配置文件
This operation will take several minutes, please wait......
Info: Succeeded in setting the file for booting system
<R1>display startup          --显示下一次启动加载的配置文件
MainBoard:
  Startup system software:                    null
  Next startup system software:               null
  Backup system software for next startup: null
  Startup saved-configuration file:       flash:/vrpcfg.zip
  Next startup saved-configuration file: flash:/backup.zip   --下一
次启动的配置文件
```

设置了下一次启动的配置文件后，再保存当前配置时，默认会将当前配置保存到所设置的下一次启动的配置文件中，从而覆盖了下次启动的配置文件的原有内容。周期性保存配置和定时保存配置，也会保存到指定的下一次启动的配置文件。

4.6.4 文件管理

VRP通过文件系统来对设备上的所有文件（包括设备的配置文件、系统文件、License文件、补丁文件）和目录进行管理。VRP文件系统主要用于创建、删除、修改、复制和显示文件及目录，这些文件和目录都存储于设备的外部存储器中。华为路由器支持的外部存储器一般有Flash和SD卡，交换机支持的外部存储器一般有Flash和CF卡。

设备的外部存储器中的文件类型是多种多样的，除了之前提到过的配置文件，还有系统软件文件、License文件、补丁文件等。在这些

文件中，系统软件文件具有特别的重要性，因为它其实就是设备的VRP操作系统本身。系统软件文件的扩展名为“.cc”，并且必须存放在外部存储器的根目录下。设备上电时，系统软件文件的内容会被加载至内存并运行。

下面就以备份配置文件为例，展示文件管理的过程。

（1）查看当前路径下的文件，并确认需要备份的文件名称与大小。

dir [/all] [*filename* | *directory*]命令可用来查看当前路径下的文件，all表示查看当前路径下的所有文件和目录，包括已经删除至回收站的文件。*filename*表示待查看文件的名称，*directory*表示待查看目录的路径。

路由器的默认外部存储器为Flash，执行如下命令可查看路由器R1的Flash存储器的根目录下的文件和目录。

```
<R1>dir  --列出当前目录文件和文件夹
Directory of flash:/
  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  drw-                 -   May 01 2018 02:51:18   dhcp --d代
表这是一个文件夹
    1  -rw-           121,802   May 26 2014 09:20:58
portalpage.zip
    2  -rw-             2,263   May 01 2018 08:13:21
statemach.efs
    3  -rw-           828,482   May 26 2014 09:20:58   sslvpn.zip
    4  -rw-               408   May 01 2018 07:27:28   private-
data.txt
    5  -rw-               897   May 01 2018 08:18:00   backup.zip
    6  -rw-               872   May 01 2018 07:27:28   vrpcfg.zip

1,090,732 KB total (784,452 KB free)
```

从回显信息中，我们看到了名为“vrpcfg.zip”的配置文件，大小为872字节，假设它就是我们需要备份的配置文件。

（2）新建目录。

创建目录的命令为mkdir *directory*, *directory*表示需要创建的目录。在Flash的根目录下创建一个名为backup的目录。

```
<R1>mkdir /backup --创建一个文件夹
Info: Create directory flash:/backup......Done
```

（3）复制并重命名文件。

复制文件的命令为copy *source-filenames destination-filename*，*source-filenames*表示被复制文件的路径及源文件名，*destination-filename*表示目标文件的路径及目标文件名。把需要备份的配置文件vrpcfg.zip复制到新目录backup下，并重命名为cfgbak.zip。

```
<R1>copy vrpcfg.zip flash:/backup/cfgbak.zip   --将vrpcfg.zip复制到
backup文件夹
Copy flash:/vrpcfg.zip to flash:/backup/cfgbak.zip? (y/n)[n]:y
100%  complete
Info: Copied file flash:/vrpcfg.zip to
flash:/backup/cfgbak.zip...Done
```

（4）查看备份后的文件。

cd directory命令用来修改当前的工作路径。我们可以执行如下操作来查看文件备份是否成功。

```
<R1>dir flash:/backup/    --列出Flash:/backup目录内容
Directory of flash:/backup/
  Idx  Attr     Size(Byte)  Date         Time(LMT)     FileName
    0  -rw-             872  May 01 2018 08:58:49    cfgbak.zip
```

回显信息表明，backup目录下已经有了文件cfgbak.bak，配置文件vrpcfg.zip的备份已顺利完成。

（5）删除文件。

当设备的外部存储器的可用空间不够时，我们就很可能需要删除其中的一些无用文件。删除文件的命令为delete [/unreserved][/force] *filename*，其中/unreserved表示彻底删除指定文件，删除的文件将不可恢复；/force表示无须确认直接删除文件；*filename*表示要删除的文件名。

如果不使用/unreserved，则delete命令删除的文件将被保存到回收站中，而使用undelete命令则可恢复回收站中的文件。注意，保存到回收站中的文件仍然会占用存储器空间。reset recycle-bin命令将会彻底删除回收站中的所有文件，这些文件将被永久删除，不能再被恢复。

以下操作为删除文件，查看删除的文件，清空回收站中的文件。

```
<R1>delete backup.zip --删除文件
Delete flash:/backup.zip? (y/n)[n]:y
Info: Deleting file flash:/backup.zip...succeed.
<R1>dir /all --参数all，显示所有文件，包括回收站中的文件
Directory of flash:/
  Idx  Attr   Size(Byte)  Date         Time(LMT)     FileName
    0  drw-             -  May 01 2018 02:51:18    dhcp
    1  -rw-       121,802  May 26 2014 09:20:58
```

```
portalpage.zip
    2  drw-                -  May 01 2018 08:58:49   backup
    3  -rw-            2,263  May 01 2018 08:13:21   statemach.efs
    4  -rw-          828,482  May 26 2014 09:20:58   sslvpn.zip
    5  -rw-              408  May 01 2018 07:27:28   private-
data.txt
    6  -rw-              872  May 01 2018 07:27:28   vrpcfg.zip
    7  -rw-              897  May 01 2018 09:11:32   [backup.zip]
--回收站中的文件

1,090,732 KB total (784,440 KB free)
<R1>reset recycle-bin  --清空回收站
Squeeze flash:/backup.zip? (y/n)[n]:y
Clear file from flash will take a long time if needed...Done.
%Cleared file flash:/backup.zip.
```

使用move命令移动文件。

```
<R1>move backup.zip flash:/backup/backup1.zip
```

进入backup目录。

```
<R1>cd backup/
```

使用pwd显示当前目录。

```
<R1>pwd
flash:/backup
```

在同一个目录中可以使用move命令，以下命令将backup1.zip重命名为backup2.zip。

```
<R1>move backup1.zip backup2.zip
```

4.6.5 将配置导出到FTP或TFTP服务器

简易文件传输协议（Trivial File Transfer Protocol，TFTP）是TCP/IP中一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务，端口号为69。此协议专门为小文件传输而设计的。因此它不具备FTP的许多功能，它只能从文件服务器上获得或写入文件，不能列出目录，不进行认证。

下面的操作将演示如何把路由器的配置文件备份到TFTP。在物理机上运行TFTP，单击“查看”→“选项”，如图4-19所示。如图4-20所示，在出现的“选项”对话框中指定“TFTP服务器根目录”，上传的文件就保存在根目录中。

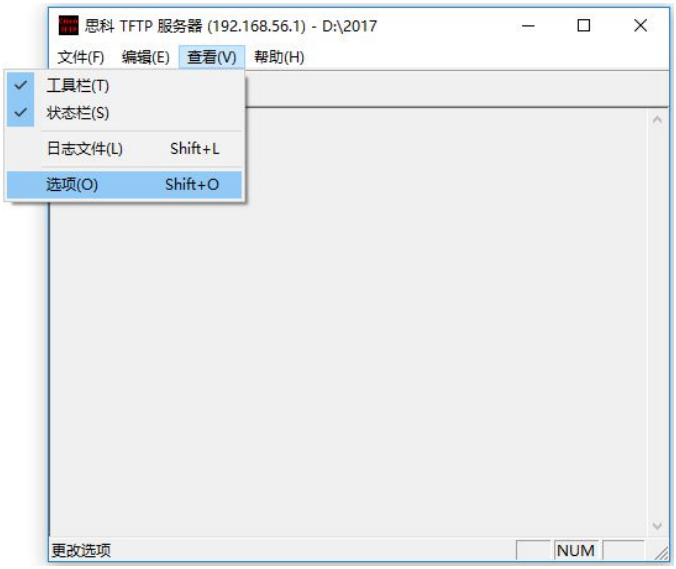


图4-19　单击“查看”→“选项”

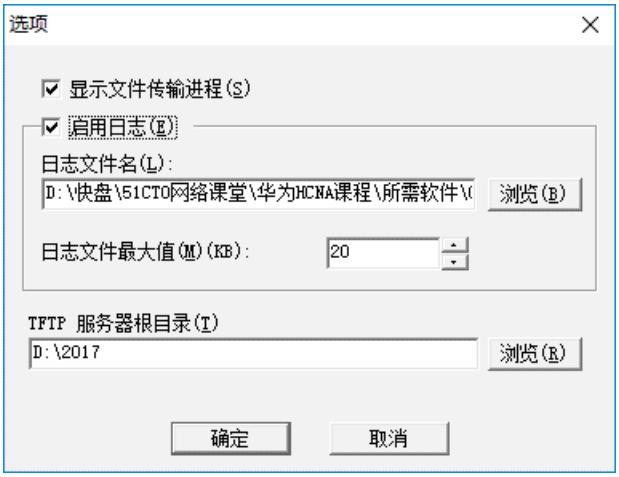


图4-20 “选项”对话框

确保R1路由器和物理机之间的网络畅通。通过执行以下命令将配置文件上传到TFTP。

```
<R1>tftp 192.168.1.11 put vrpcfg.zip vrpcfg.zip     --将配置文件上传到TFTP
<R1>tftp 192.168.1.11 get vrpcfg.zip backup.zap     --从TFTP下载配置文件
```

put和get命令后面跟的是源文件名和目标文件名。

TFTP的安全性差，任何用户都可以接入TFTP进行文件的上传和下载。而使用FTP就需要进行身份验证，因而比TFTP安全。

下面在Windows 10上安装FTP服务。

打开控制面板，单击“程序”，出现的页面如图4-21所示，在“程序”对话框中单击“启用或关闭Windows功能”选项。

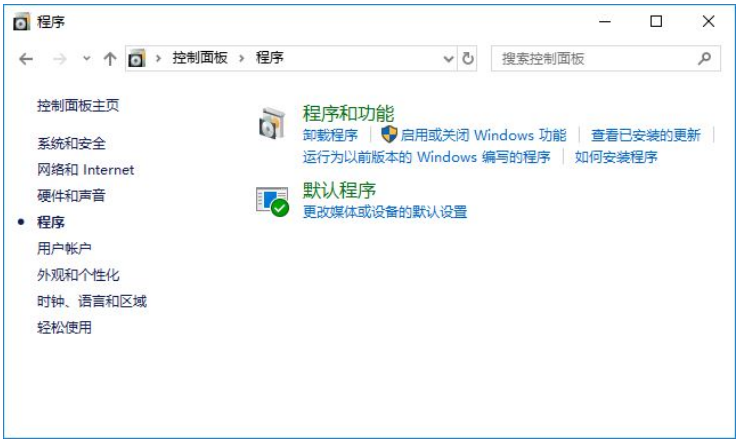


图4-21　启用或关闭Windows功能

“Windows功能”对话框出现，如图4-22所示，选中“FTP服务器”下的“FTP服务”，单击“确定”按钮。

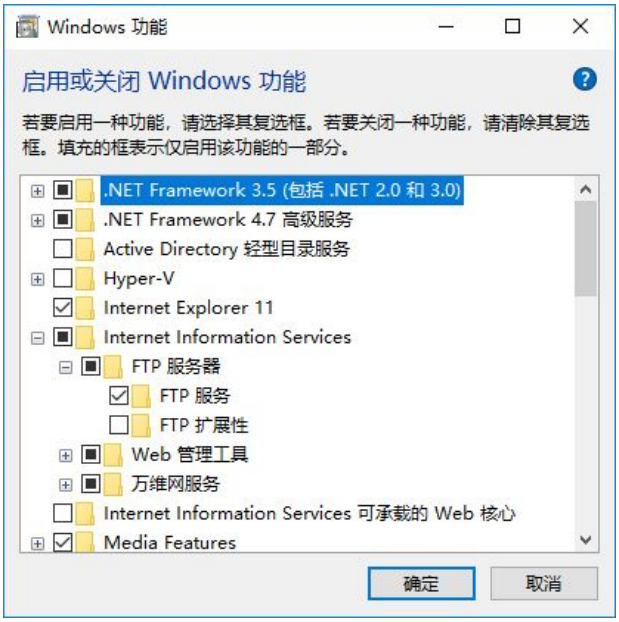


图4-22　选中“FTP服务”

打开IIS管理器，如图4-23所示，右键单击“网站”，在弹出的菜单中单击“添加FTP站点”。

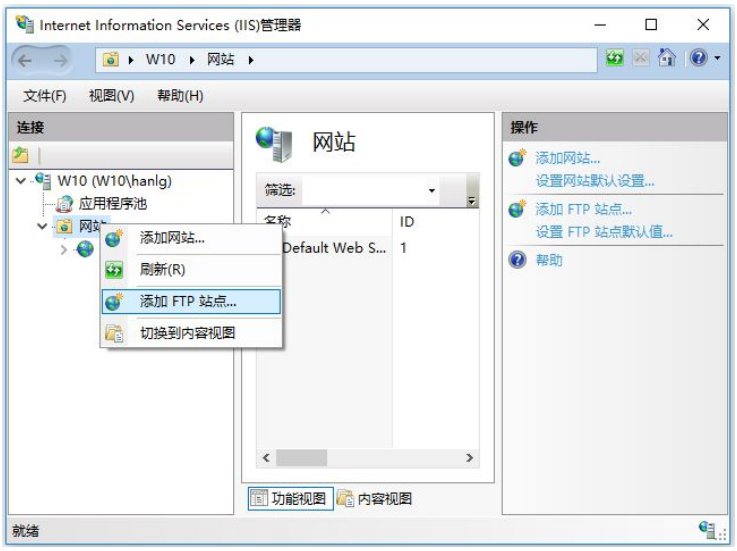


图4-23　添加FTP站点

如图4-24所示，在出现的设置站点信息对话框中指定“FTP站点名称”和“物理路径”，单击“下一步”按钮。

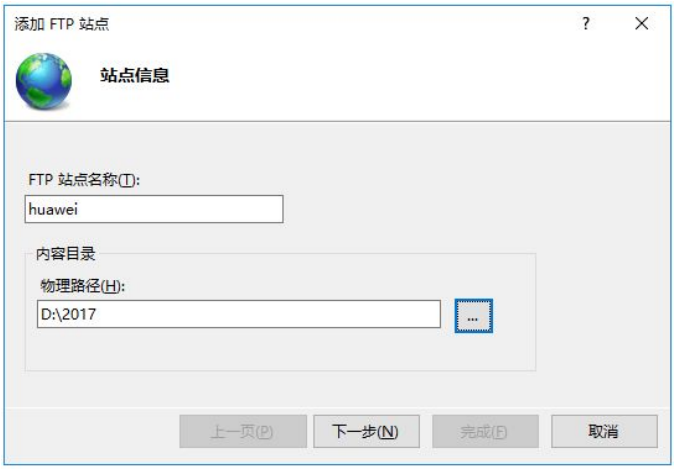


图4-24　设置FTP站点信息

如图4-25所示，在出现的“绑定和SSL设置”对话框中，为“IP地址”选择“全部未分配”，选中“自动启动FTP站点”，为“SSL”选择“无SSL”，单击“下一步”按钮。

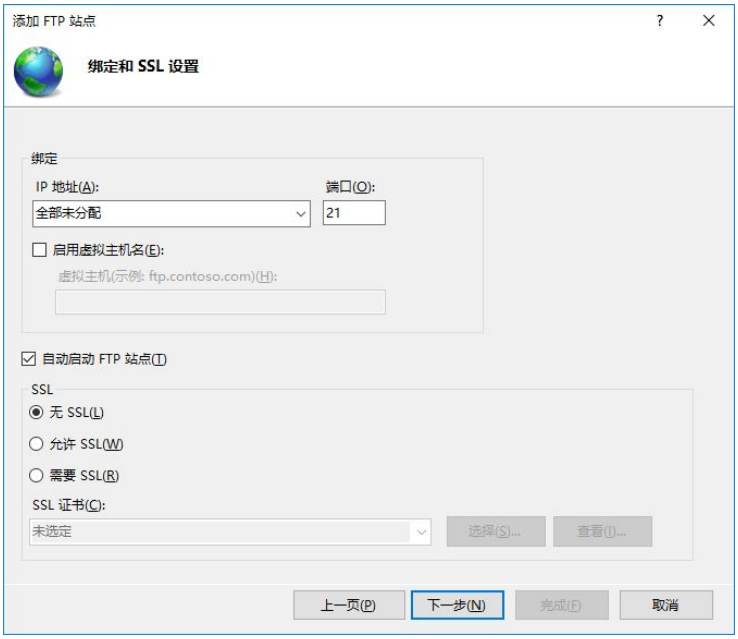


图4-25　指定使用的地址

如图4-26所示，在出现的“身份验证和授权信息”对话框中，选中“基本”，设置允许所有用户读写，再单击“完成”按钮。将来访问FTP站点的账户就可以使用计算机账户了。

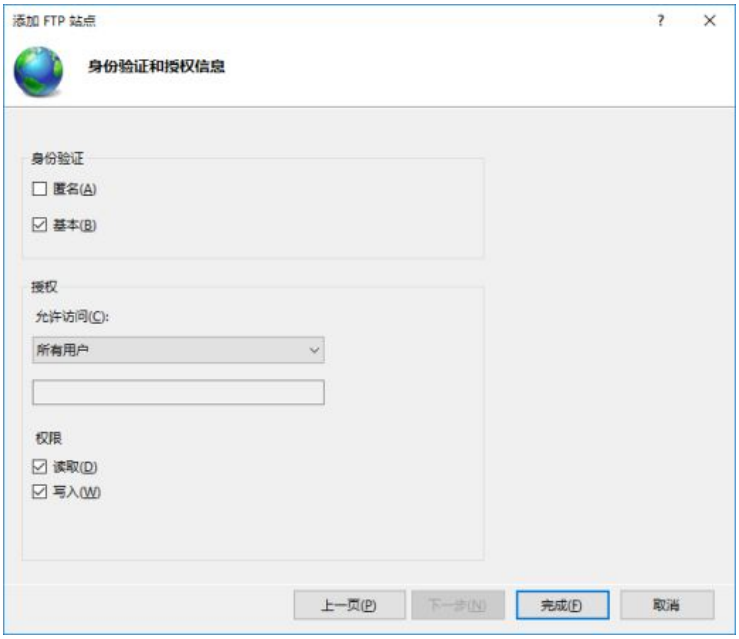


图4-26　设置身份验证和授权信息

打开Windows命令提示符，输入wf.msc，按回车键后，Windows高级防火墙设置界面被打开。如图4-27所示，可以看到公用配置文件是活动的，单击“Windows Defender防火墙属性”。

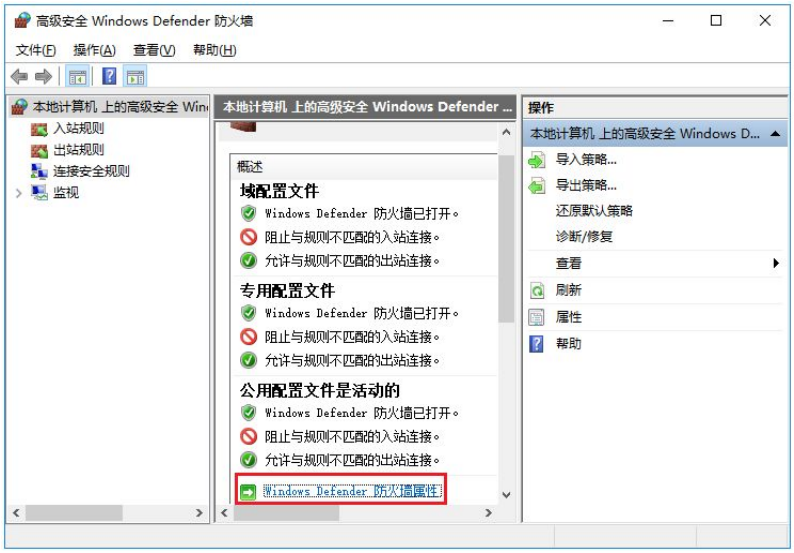


图4-27　打开防火墙属性界面

如图4-28所示，在出现的防火墙属性对话框中，在“公用配置文件”选项卡下，为“防火墙状态”选择“关闭”。

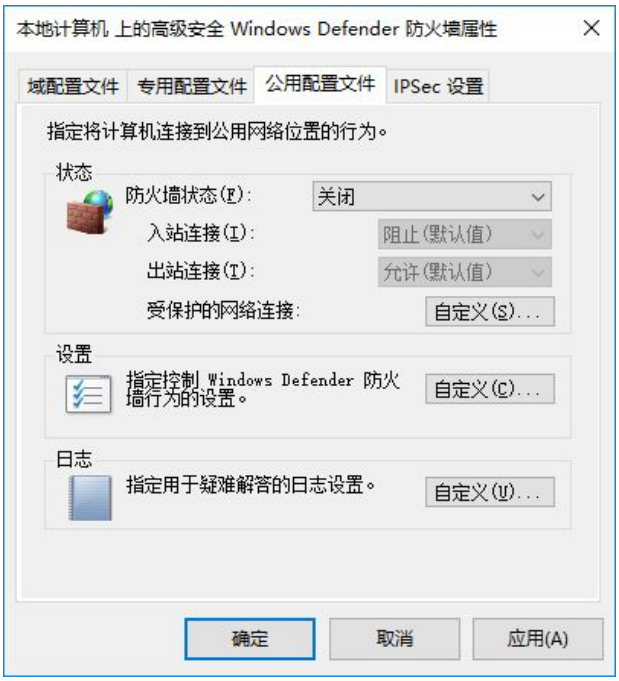


图4-28　关闭防火墙

在路由器R1上将配置上传到FTP服务器。

```
<R1>ftp 192.168.1.11
Trying 192.168.1.11 ...
Press CTRL+K to abort
Connected to 192.168.1.11.
220 Microsoft FTP Service
User(192.168.1.11:(none)):han                    --输入用户名
331 Password required                            --输入密码
Enter password:
230 User logged in.
[R1-ftp]put vrpcfg.zip vrpcfg.zip.bak            --上传vrpcfg.zip到FTP
服务器
[R1-ftp]dir    --查看FTP目录的内容
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-01-18  11:50PM                  872 vrpcfg.zip.bak    --上传的文
件
226 Transfer complete.
FTP: 55 byte(s) received in 0.020 second(s) 2.75Kbyte(s)/sec.

[R1-ftp]get vrpcfg.zip.bak vrpcfg2.zip  --从FTP服务器下载文件
vrpcfg.zip.bak
```

4.7 习题

1. 下面哪个是更改路由器名称的命令？（　　）

A. < Huawei > sysname R1

B. [Huawei]sysname R1

C. [Huawei]system R1

D. < Huawei > system R1

2. 本章eNSP模拟软件需要和哪两款软件一起安装？（　　）

A. Wireshark和VMWareWorkstation

B. Wireshark和VirtualBox

C. VirtualBox和VMWareWorkstation

D. VirtualBox和Ethereal

3. 给路由器接口配置IP地址，下面哪条命令是错误的？（　　）

A. [R1]ip address 192.168.1.1 255.255.255.0

B. [R1-GigabitEthernet0/0/0]ip address 192.168.1.1 24

C. [R1-GigabitEthernet0/0/0]ip add 192.168.1.1 24

D. [R1-GigabitEthernet0/0/0]ip address 192.168.1.1 255.255.255.0

4. 查看路由器当前配置的命令（　　）。

A. <R1>display current-configuration

B. <R1>display saved-configuration

C. [R1-GigabitEthernet0/0/0]display

D. [R1]show current-configuration

5. 华为路由器保存配置的命令（　　）。

A. [R1]save

B. <R1>save

C. <R1>copy current startup

D. [R1] copy current startup

6. 更改路由器下一次启动加载的配置文件使用哪个命令？（　　）

A. <R1>startup saved-configuration backup.zip

B. <R1>display startup

C. [R1]startup saved-configuration

D. [R1]display startup

7. 配置路由器的console口只需要密码验证，需要执行以下哪条命令？（　　）

A. [R1-ui-console0]authentication-mode password

B. [R1-ui-console0]authentication-mode aaa

C. [R1-ui-console0]authentication-mode Radius

D. [R1-ui-console0]authentication-mode scheme

8. 在路由器上创建用户han，允许通过Telnet配置路由器，且用户权限级别为3，需要执行哪两条命令？（　　）

A. [R1-aaa]local-user han password cipher 91xueit3 privilege level 3

B. [R1-aaa]local-user han service-type telnet

C. [R1-aaa]local-user han password cipher 91xueit3

D. [R1-aaa]local-user hanservice-type terminal

9. 在系统视图下键入什么命令可以切换到用户视图？（　　）

A. system-view

B. router

C. quit

D. user-view

10. 管理员想要彻底删除旧的设备配置文件config.zip，则下面的命令正确的是（　　）。

A. delete /force config.zip

B. delete /unreserved config.zip

C. reset config.zip

D. clear config.zip

11. 华为AR路由器的命令行界面下，Save命令的作用是保存当前的系统时间。（　　）

A. 正确　　B. 错误

12. 保存路由器的配置文件时，一般是保存在下面哪种储存介质上？（　　）

A. SDRAM

B. NVRAM

C. Flash

D. Boot ROM

13. VRP的全称是什么？（　　）

A. Versatile Routine Platform

B. Virtual Routing Platform

C. Virtual Routing Plane

D. Versatile Routing Platform

14. VRP操作系统命令划分为访问级、监控级、配置级、管理级4个级别。能运行各种业务配置命令但不能操作文件系统的是哪一级？（　　）

A. 访问级

B. 监控级

C. 配置级

D. 管理级

15. 管理员在哪个视图下才能为路由器修改设备名称？（　　）

A. User-view

B. System-view

C. Interface-view

D. Protocol-view

16. 目前，公司有一个网络管理员，公司网络中的AR2200通过Telent直接输入密码后就可以实现远程管理。新来了两个管理员后，公司希望给所有的管理员分配各自的用户名和密码，以及不同的权限等级。那么应该如何操作呢？（　　）（选择3个答案）

A. 在AAA视图下配置3个用户名和各自对应的密码

B. Telent配置的用户认证模式必须为AAA模式

C. 在配置每个管理员的账户时，需要配置不同的权限级别

D. 每个管理员在运行Telent命令时，使用设备的不同公网IP地址

17. VRP支持通过哪几种方式对路由器进行配置？（　　）（选择3个答案）

A. 通过Console口对路由器进行配置

B. 通过Telent对路由器进行配置

C. 通过mini USB口对路由器进行配置

D. 通过FTP对路由器进行配置

18. 操作用户成功Telnet到路由器后，无法使用配置命令配置接口IP地址，可能的原因有（　　）。

A. 操作用户的Telnet终端软件不允许用户对设备的接口配置IP地址

B. 没有正确设置Telnet用户的认证方式

C. 没有正确设置Telnet用户的级别

D. 没有正确设置SNMP参数

19. 关于下面的display信息描述正确的是（　　）。

[R1]display interface g0/0/0 GigabitEthernet0/0/0 current state:Administratively DOWN Line protocol current state:DOWN

A. Gigabit Ethernet 0/0/0 接口连接了一条错误的线缆

B. Gigabit Ethernet 0/0/0接口没有配置IP地址

C. Gigabit Ethernet 0/0/0接口没有启用动态路由协议

D. Gigabit Ethernet 0/0/0接口被管理员手动关闭了

20．路由器上电时，会从默认存储路径中读取配置文件进行路由器的初始化工作。如果默认存储路径中没有配置文件，则路由器会使用什么来进行初始化？

A．当前配置

B．新建配置

C．默认参数

D．起始配置

第5章　静态路由

本章内容

- 路由基础
- 路由汇总
- 默认路由
- 网络排错案例

路由器负责在不同网段间转发数据包，根据路由表为数据包选择转发路径。路由表中有多条路由信息，一条路由信息也被称为一个路由项或一个路由条目，一个路由条目记录一个网段的路由。路由条目可以由管理员用命令输入，称为静态路由；也可以由路由协议（RIP、OSPF协议）生成，称为动态路由。路由表中的条目可以由动态路由和静态路由组成。

本章将讲述网络畅通的条件，给路由器配置静态路由的方法，如何合理规划IP地址以使用路由汇总和默认路由从而简化路由表。

本章还讲解了排除网络故障的方法，使用ping命令测试网络是否畅通，使用pathping和tracert命令跟踪数据包的路径。同时也讲解Windows操作系统中的路由表，给Windows系统添加路由的方式。

本章只讲静态路由，第6章介绍动态路由。

5.1　路由基础

5.1.1　什么是路由

在网络通信中，“路由”（route）是网络层的一个术语，它是指从某一网络设备出发去往某个目的地的路径。网络中的路由器（或三层交换机）负责为数据包选择转发路径。如图5-1所示，路由器中有路由表（routing table），路由表是若干条路由信息的一个集合体。在路由表中，一条路由信息也被称为一个路由项或一个路由条目，路由器根据路由表为数据包选择转发路径。路由表只存在于终端计算机和路由器（以及三层交换机）中，二层交换机中是不存在路由表的。

如图5-1所示，PC1给PC2发送一个数据包，源IP地址是11.1.1.2，目标IP地址是12.1.1.2。R1路由器收到该数据包，查路由表发现有到12.1.1.0/24网段的路由，下一跳是172.16.0.2，于是该数据包就从R1路由器的GE 0/0/0接口发送给R2路由器。R2路由器收到后查看路由表，发现有到12.1.1.0/24网段的路由，下一跳是172.16.1.2，于是该数据包就从R2路由器的GE 0/0/1接口发送给R3路由器。R3路由器收到该数据包后查路由表，发现有到12.1.1.0/24网段的路由，下一跳是12.1.1.1，该地址是R3路由器GE 0/0/1接口的地址，该数据包就从GE 0/0/1发送出去，最终到达PC2。PC2给PC1发送数据包，也需要沿途路由器查询路由表以决定转发路径。

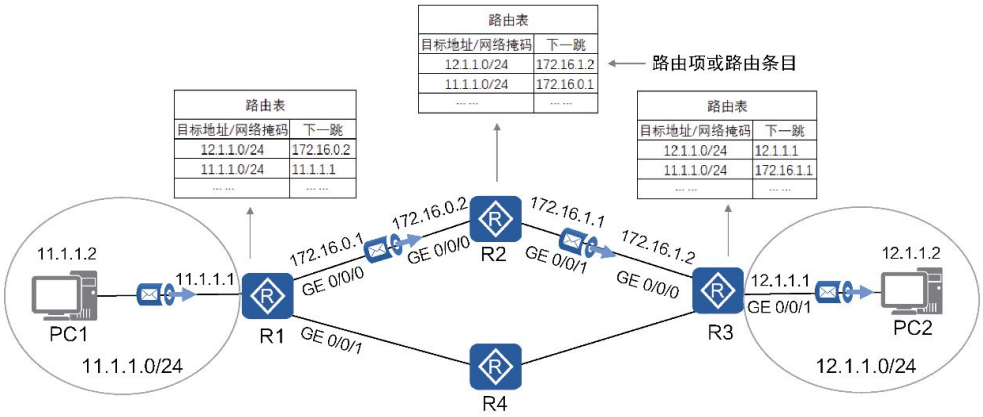


图5-1　IP路由

需要指出的是，如果一个路由项的下一跳IP地址与出接口的IP地址相同，则说明出接口已经直连到了该路由项所指的目的网络（也就是说，出接口已经位于目的网络之中了）。还需要指出的是，下一跳IP地址所对应的那个主机接口与出接口一定是位于同一个二层网络（二层广播域）中。

下面是实际路由器上的路由表，输入display ip routing-table便可看到路由表。可以看到该路由表有14个目标网段（destination）、14条路由（route）。

```
[AR1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

            ......
    172.16.0.0/24   Direct  0    0           D   172.16.0.1      Serial2/0/0
    172.16.0.2/32   Direct  0    0           D   172.16.0.2      Serial2/0/0
    172.16.1.0/24   OSPF    10   96          D   172.16.0.2
```

```
Serial2/0/0
    192.168.0.0/24  Direct   0     0           D    192.168.0.1
Vlanif1
    192.168.1.0/24  OSPF     10    97          D    172.16.0.2
Serial2/0/0
   192.168.10.0/24  Static   60    0           RD   172.16.0.2
Serial2/0/0
            ......
```

下面对路由条目的各个字段进行解释。

- Destination/Mask表示目标网段和子网掩码。
- Proto即Protocol（协议）的简写，表明该路由条目是通过什么协议生成的。Direct是直连网段，即自动发现的路由。OSPF表明该路由条目是通过OSPF协议构建的动态路由，Static表明该路由条目是手动配置的静态路由。
- Pre即Preference（优先级）的简写，用来反映路由信息来源的优先级。
- Cost表示开销，路由的开销是路由的一个非常重要的属性，路由器为数据包选择最佳转发路径，最佳路径也就是开销小的路径。
- Flags表示路由标记，R表示该路由是迭代路由，D表示该路由下发到FIB表。
- NextHop表示下一跳，即到达目标网段。路由器通过下一跳就能够断定该数据包应该从哪个接口发送出去。
- Interface表示到达目标网段的下一跳出口。

5.1.2 路由信息的来源

路由表包含了若干条路由信息，这些路由信息的生成方式总共有 3 种：设备自动发现、手动配置、通过动态路由协议生成，这 3 种方式生成的路由分别叫作直连路由、静态路由和动态路由。

1. 直连路由

我们把设备自动发现的路由信息称为直连路由（Direct Route）。网络设备启动之后，如果接口配置了IP地址和子网掩码，当接口状态为UP时，路由器就能够自动发现接口所在网段，并把该网段添加到路由表。

如图5-2所示，路由器R1的GE 0/0/1接口的状态为UP时，R1便可以根据GE 0/0/1接口的IP地址11.1.1.1/24推断出GE 0/0/1接口所在网络的网络地址为11.1.1.0/24。于是，R1便会将11.1.1.0/24作为一个路由项填进自己的路由表，这条路由的目的地/掩码为11.1.1.0/24，出接口为GE 0/0/1，下一跳的IP地址是与出接口的IP地址相同的，即11.1.1.1。由于这条路由是直连路由，所以其Protocol属性为Direct。另外，对于直连路由，其cost的值总是为0。

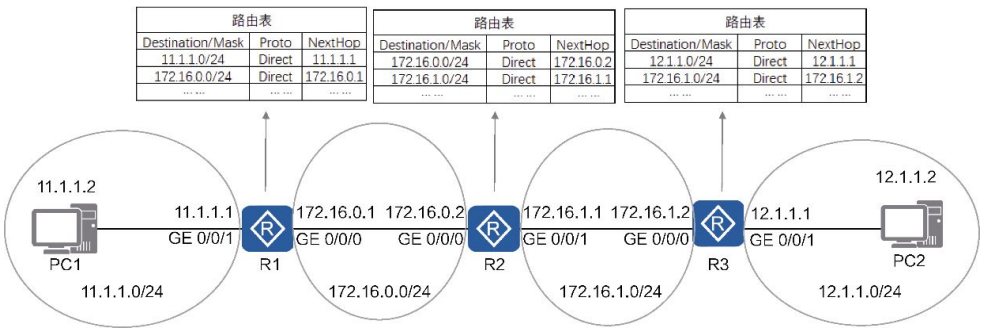


图5-2　直连路由

类似，路由器R1还会自动发现另外一条直连路由，该路由的目的地/掩码为172.16.0.0/24，出接口为GE 0/0/0，下一跳地址是172.16.0.1，Protocol属性为Direct，Cost的值为0。

可以看到当网络中的R1、R2、R3路由器开机，且端口状态UP时，这些端口连接的网段就会出现在路由表中。

2. 静态路由

要想让网络中的计算机能够访问任何网段，那么网络中的路由器必须有到全部网段的路由。对于路由器直连的网段，路由器能够自动发现它并将其加入到路由表。对于没有直连的网络，管理员需要手动添加到这些网段的路由。在路由器上手动配置的路由信息被称为静态路由（Static Route），它适合规模较小的网络或网络不怎么变化的情况。

如图5-3所示，网络中有4个网段，每个路由器直连两个网段，对于没有直连的网段，需要手动添加静态路由。我们需要在每个路由器上添加两条静态路由。注意观察静态路由的下一跳，在R1上添加到12.1.1.0/24网段的路由，下一跳是172.16.0.2，而不是R3的GE0/0/0接口的172.16.1.2。很多初学者对“下一跳”的理解会出现错误。

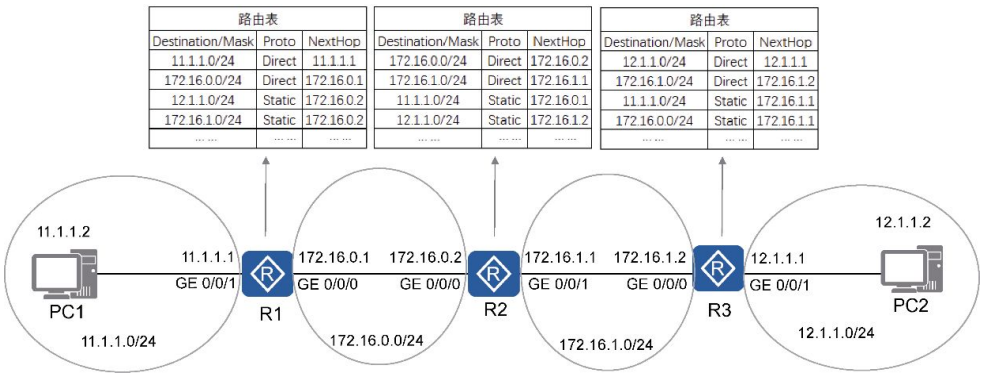


图5-3　手动配置静态路由

3. 动态路由

路由器使用动态路由协议（RIP、OSPF）而获得路由信息被称为动态路由（Dynamic Route）。动态路由适合规模较大的网络，能够针对网络的变化自动选择最佳路径。

如果网络规模不大，我们可以通过手动配置的方式“告诉”网络设备去往哪些非直接相连的网络的路由。然而，如果非直接相连的网络的数量众多，必然会耗费大量的人力来进行手动配置，这在现实中往往是不可取的，甚至是不可能的。另外，手动配置的静态路由还有一个明显的缺陷，就是它不具备自适应性。当网络发生故障或网络结构发生改变而导致相应的静态路由发生错误或失效时，必须手动对这些静态路由进行修改，而这在现实中也往往是不可取的，或是不可能的。

事实上，网络设备还可以通过运行路由协议来获取路由信息。“路由协议”和“动态路由协议”这两个术语其实是一回事，这是因为我们还未曾有过被称为“静态路由协议”的路由协议（我们有静态路由，但无静态路由协议）。网络设备通过运行路由协议而获取到的路由称为动态路由。如果网络新增了网段、删除了网段、改变了某个接口所在的网段，或网络拓扑发生了变化（网络中断了一条链路或增加了一条链路），那么路由协议能够及时地更新路由表中的胴体路由信息。

需要特别指出的是，一台路由器是可以同时运行多种路由协议的。如图5-4所示，R2路由器同时运行RIP路由协议和OSPF路由协议。此时，该路由器除了会创建并维护一个IP路由表，还会分别创建并维护一个RIP路由表和一个OSPF路由表。RIP路由表用来专门存放RIP发现的所有路由，OSPF路由表用来专门存放OSPF协议发现的所有路由。

RIP路由表和OSPF路由表中的路由项都会加进IP路由表中，如果RIP路由表和OSPF路由表都有到某一网段的路由项，那就要比较路由协议优先级了。在图5-4中，R2路由器的RIP路由表和OSPF路由表都有24.6.10.0/24网段的路由信息，由于OSPF协议的优先级高于RIP，所以OSPF路由表中的24.6.10.0/24路由项被加进IP路由表。而路由器最终是根据IP路由表来进行IP报文的转发工作的。

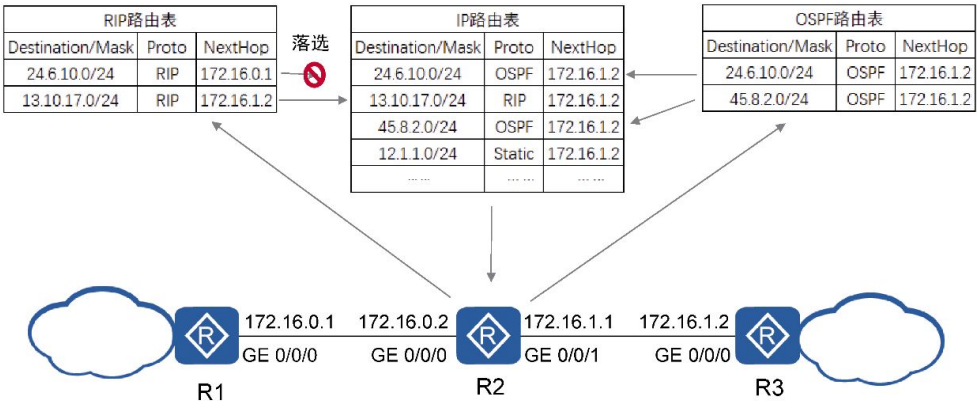


图5-4　动态路由优先级

5.1.3　路由优先级

假设一台华为AR路由器同时运行了RIP和OSPF这两种路由协议，RIP发现了一条去往目的地/掩码为z/y的路由，OSPF也发现了一条去往

目的地/掩码为z/y的路由。另外，我们还手动配置了一条去往目的地/掩码为z/y的路由。也就是说，该设备同时获取了去往同一目的地/掩码的三条不同的路由，那么该设备究竟会采用哪一条路由来进行IP报文的转发呢？或者说，这三条路由中的哪一条会被加入IP路由表呢？

事实上，我们给不同来源的路由规定了不同的优先级（preference），并规定优先级的值越小，则路由的优先级就越高。这样，当存在多条目的地/掩码相同，但来源不同的路由时，则具有最高优先级的路由便成为了最优路由，并被加入IP路由表中，而其他路由则处于未激活状态，不显示在IP路由表中。

设备上的路由优先级一般都具有默认值。不同厂家的设备对于优先级的默认值的规定可能不同。华为AR路由器上部分路由优先级的默认值的规定如表5-1所示。这些都是默认的优先级。我们可以更改优先级，比如添加静态路由时指定该静态路由的优先级。

表5-1　路由的优先级

路由来源	优先级的默认值
直连路由	0
OSPF	10
静态路由	60

路由来源	优先级的默认值
RIP	100
BGP	255

5.1.4　网络畅通的条件

计算机网络畅通的条件就是数据包能去能回，道理很简单，却是我们排除网络故障的理论依据。

如图5-5所示，网络中的计算机A要想实现和计算机B通信，沿途的所有路由器必须有到目标网络192.168.1.0/24的路由。计算机B给计算机A返回数据包，途径的所有路由器必须到达192.168.0.0/24网段的路由。

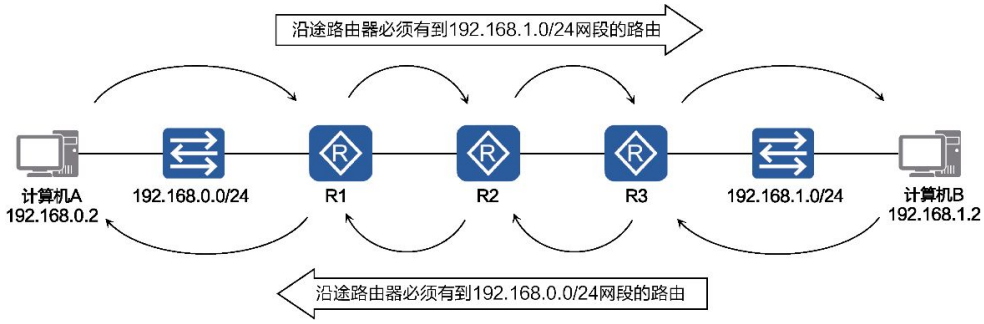


图5-5　网络畅通的条件

基于以上原理，网络排错就变得简单了。如果网络不通，就要检查计算机是否配置了正确的IP地址子网掩码以及网关，首先逐一检查

沿途路由器上的路由表，查看是否有到达目标网络的路由；然后逐一检查沿途路由器上的路由表，检查是否有数据包返回所需的路由。

5.1.5 配置静态路由示例

下面就通过一个案例来学习静态路由的配置，网络拓扑如图5-6所示，设置网络中的计算机和路由器接口的IP地址，PC1和PC2都要设置网关。可以看到，该网络中有4个网段。现在需要在路由器上添加路由，实现这4个网段间网络的畅通。

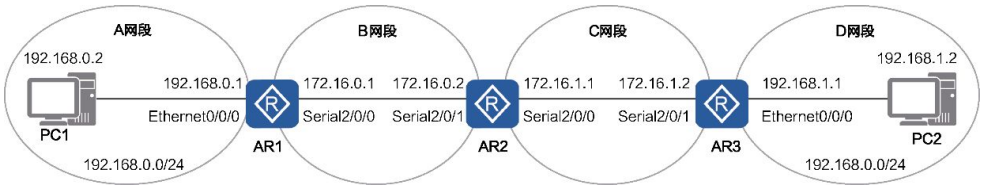


图5-6 静态路由网络拓扑

前面讲过，只要给路由器接口配置了IP地址和子网掩码，路由器的路由表就有了到直连网段的路由，不需要再添加到直连网段的路由。在添加静态路由之前先看看路由器的路由表。

在AR1路由器上，进入系统视图，输入命令display ip routing-table可以看到两个直连网段的路由。

```
[AR1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
```

```
   127.0.0.1/32  Direct 0   0      D   127.0.0.1  InLoopBack0
127.255.255.255/32  Direct 0  0    D   127.0.0.1     InLoopBack0
   172.16.0.0/24  Direct 0  0      D   172.16.0.1  Serial2/0/0
--直连网段路由
     172.16.0.1/32  Direct  0    0        D   127.0.0.1
Serial2/0/0
     172.16.0.2/32  Direct  0    0        D   172.16.0.2
Serial2/0/0
   172.16.0.255/32  Direct  0    0        D   127.0.0.1
Serial2/0/0
    192.168.0.0/24  Direct  0    0        D   192.168.0.1
Vlanif1--直连网段路由
    192.168.0.1/32  Direct  0    0        D   127.0.0.1
Vlanif1
  192.168.0.255/32  Direct  0    0        D   127.0.0.1
Vlanif1
255.255.255.255/32  Direct  0    0        D   127.0.0.1
InLoopBack0
```

可以看到路由表中已经有了到两个直连网段的路由条目。

在路由器AR1、AR2和AR3上添加静态路由。

（1）在路由器AR1上添加到172.16.1.0/24、192.168.1.0/24网段的路由，并显示添加的静态路由。

```
[AR1]ip route-static 172.16.1.0 24 172.16.0.2        --添加静态路
由、下一跳地址
[AR1]ip route-static 192.168.1.0 255.255.255.0 Serial 2/0/0   --添
加静态路由、出口
[AR1]display ip routing-table                         --显示路由表
[AR1]display ip routing-table protocol static         --只显示静态路
由表
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------
-----------
Public routing table : Static
      Destinations : 2      Routes : 2        Configured Routes :
2
Static routing table status : <Active>
      Destinations : 2      Routes : 2
Destination/Mask    Proto   Pre  Cost      Flags   NextHop
Interface
```

```
   172.16.1.0/24  Static 60   0      RD    172.16.0.2
Serial2/0/0
  192.168.1.0/24  Static 60   0       D    172.16.0.1
Serial2/0/0
Static routing table status : <Inactive>
       Destinations : 0        Routes : 0
```

（2）在路由器AR2上添加到192.168.0.0/24、192.168.1.0/24网段的路由。

```
[AR2]ip route-static 192.168.0.0 24 172.16.0.1
[AR2]ip route-static 192.168.1.0 24 172.16.1.2
```

（3）在路由器AR3上添加到192.168.0.0/24、172.16.0.0/24网段的路由。

```
[AR3]ip route-static 192.168.0.0 24 172.16.1.1
[AR3]ip route-static 172.16.0.0 24 172.16.1.1
```

在R2路由器上删除到192.168.1.0/24网络的路由。

```
[AR2]undo ip route-static 192.168.1.0 24     --删除到某个网段的路由，不用指定下一跳地址
```

PC1 ping PC2，显示Request timeout!（请求超时！），实际上是目标主机不可到达。

并不是所有的“请求超时”都是路由器的路由表造成的，其他的原因也可能导致请求超时，比如对方的计算机启用防火墙或对方的计算机关机，这些都能引起“请求超时”。

5.1.6 浮动静态路由

浮动路由又称为路由备份，两条或多条链路组成浮动路由。当到达某一网络有多条路径时，通过为静态路由设置不同的优先级，你可以指定主用路径和备用路径。当主用路径不可用时，走备用路径的静态路由进入路由表，数据包通过备用路径被转发到目标网络，这就是浮动路由。

如图5-7所示，从A网段到B网段的最佳路径是从AR1AR3。当最佳路径不可用时，可以走备用路径AR1AR2AR3。这就是需要在AR1和AR3上配置浮动静态路由的原因，即为添加到同一网段的路由指定不同的优先级。指定路由优先级的参数是preference，取值1～255，值越大，优先级越低，直连网络的优先级为0，静态路由的优先级默认为60。

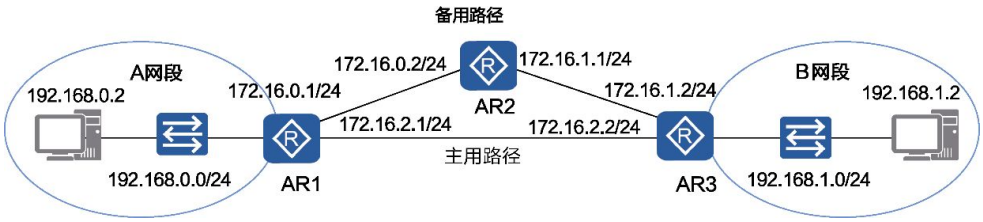


图5-7　备用路径

在AR1上添加两条到192.168.1.0/24网段的静态路由，主用路径优先级使用默认值，备用路径的静态路由优先级设置成100。

```
[AR1]ip route-static 192.168.1.0 24 172.16.2.2
[AR1]ip route-static 192.168.1.0 24 172.16.2.2 preference ?
  INTEGER<1-255>  Preference value range
[AR1]ip route-static 192.168.1.0 24 172.16.0.2 preference 100
```

在AR3上添加两条到192.168.0.0/24网段的静态路由，主用路径优先级使用默认值，备用路径的静态路由优先级设置成100。

```
[AR3]ip route-static 192.168.0.0 24 172.16.2.1
[AR3]ip route-static 192.168.0.0 24 172.16.1.1 preference 100
```

在AR2上添加到192.168.0.0/24和192.168.1.0/24网段的静态路由。

```
[AR2]ip route-static 192.168.0.0 24 172.16.0.1
[AR2]ip route-static 192.168.1.0 24 172.16.1.2
```

在AR1上查看路由表，可以看到主用路径的路由，备用路径的静态路由没有加入路由表。

```
[AR1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14    Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags  NextHop
Interface
 ......
 192.168.0.0/24     Direct   0    0         D   192.168.0.1
Vlanif1
 192.168.0.1/32     Direct   0    0         D   127.0.0.1
Vlanif1
 192.168.0.255/32   Direct   0    0         D   127.0.0.1
Vlanif1
 192.168.1.0/24     Static  60    0        RD  172.16.2.2
GigabitEthernet0/0/1
255.255.255.255/32  Direct   0    0         D   127.0.0.1
InLoopBack0
```

查看全部静态路由，此时能够显示主路由和备用路由。Active表示该路由加入了IP路由表，Inactive表示该路由没有加入IP路由表。

```
<AR1>display ip routing-table protocol static
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Public routing table : Static
```

```
        Destinations : 1        Routes : 2        Configured
Routes : 2
Static routing table status : <Active>
            Destinations : 1    Routes : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop
Interface
    192.168.1.0/24  Static  60   0         RD    172.16.2.2
GigabitEthernet0/0/1
Static routing table status : <Inactive>
             Destinations : 1     Routes : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop
Interface
    192.168.1.0/24  Static  100  0           R  172.16.0.2
GigabitEthernet0/0/0
```

在AR1上关闭主用路径的接口，再次查看路由表，可以看到备用路由生效。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]shutdown
<AR1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
……
Destination/Mask    Proto   Pre  Cost      Flags NextHop
Interface
  192.168.0.255/32  Direct  0    0         D     127.0.0.1    Vlanif1
  192.168.1.0/24  Static  100    0       RD    172.16.0.2
GigabitEthernet0/0/0
```

5.2　路由汇总

Internet是全球最大的互联网，如果Internet上的路由器把全球所有的网段都添加到路由表中，那将是一张非常庞大的路由表。路由器每转发一个数据包，都要检查路由表，并为该数据包选择转发出口。庞大的路由表势必会增加处理时延。

如果为物理位置连续的网络分配地址连续的网段，就可以在边界路由器上将远程的网段合并成一条路由，这就是路由汇总。路由汇总能够大大减少路由器上的路由表条目。

5.2.1　通过路由汇总精简路由表

下面以实例来说明如何实现路由汇总。

如图5-8所示，北京市的网络可以认为是物理位置连续的网络，为北京市的网络分配连续的网段，即从192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24、192.168.4.0/24一直到192.168.255.0/24的网段。

石家庄市的网络也可以认为是物理位置连续的网络，为石家庄市的网络分配连续的网段，即从172.16.0.0/24、172.16.1.0/24、172.16.2.0/24、172.16.3.0/24、172.16.4.0/24一直到172.16.255.0/24的网段。

在北京市的路由器中添加到石家庄市全部网段的路由，如果为每一个网段添加一条路由，需要添加256条路由。在石家庄市的路由器中添加到北京市全部网络的路由，如果为每一个网段添加一条路由，也需要添加256条路由。

石家庄市的这些子网172.16.0.0/24、172.16.1.0/24、172.16.2.0/24、…、172.16.255.0/24都属于172.16.0.0/16网段，这个网段包括全部以172.16开始的网段。因此，在北京市的路由器中添加一条到172.16.0.0/16这个网段的路由即可。

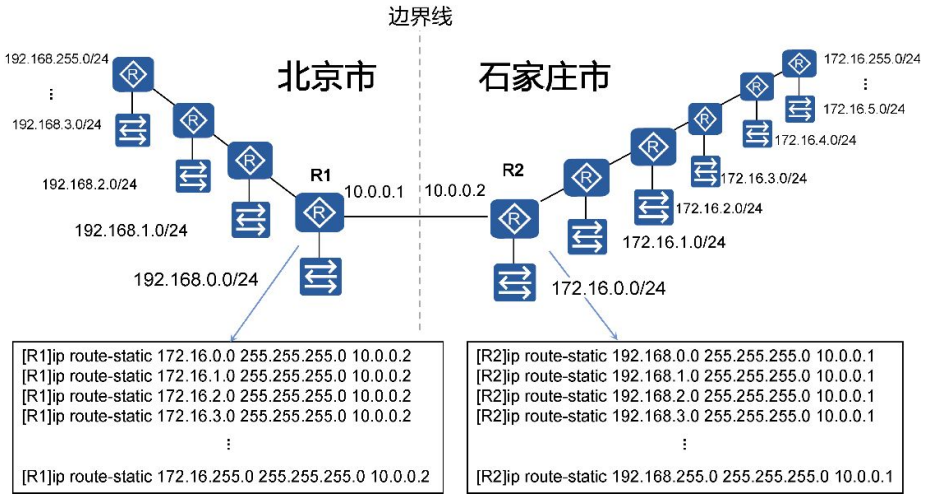


图5-8　地址规划

北京市的网段从192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24、192.168.4.0/24一直到192.168.255.0/24，也可以合并成一个网段192.168.0.0/16（这时候一定要能够想起第3章讲到的使用超网合并网段，192.168.0.0/16就是一个超网，子网掩码前移了8位，合并了 256 个 C类网络），这个网

段包括全部以192.168开始的网段。因此，在石家庄市的路由器中添加一条到192.168.0.0/16这个网段的路由即可。

汇总北京市的路由器R1中的路由和石家庄市的路由器R2中的路由后，路由表得到极大的精简，如图5-9所示。

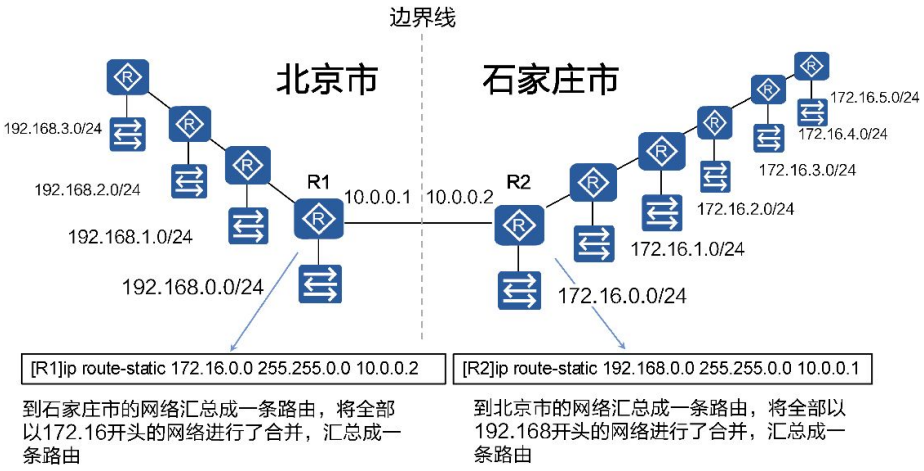


图5-9　地址规划后可以进行路由汇总

进一步，如图5-10所示，如果石家庄市的网络使用172.0.0.0/16、172.1.0.0/26、172.2.0.0/16、…、172.255.0.0/16这些网段，总之，凡是以172打头的网络都在石家庄市，那么可以将这些网段合并为一个网段172.0.0.0/8。在北京市的边界路由器R1中只需要添加一条路由即可。如果北京市的网络使用192.0.0.0/16、192.1.0.0/16、192.2.0.0/16、…、192.255.0.0/26这些网段，总之，凡是以 192 打头的网络都在北京市，那么也可以将这些网段合并为一个网段192.0.0.0/8。

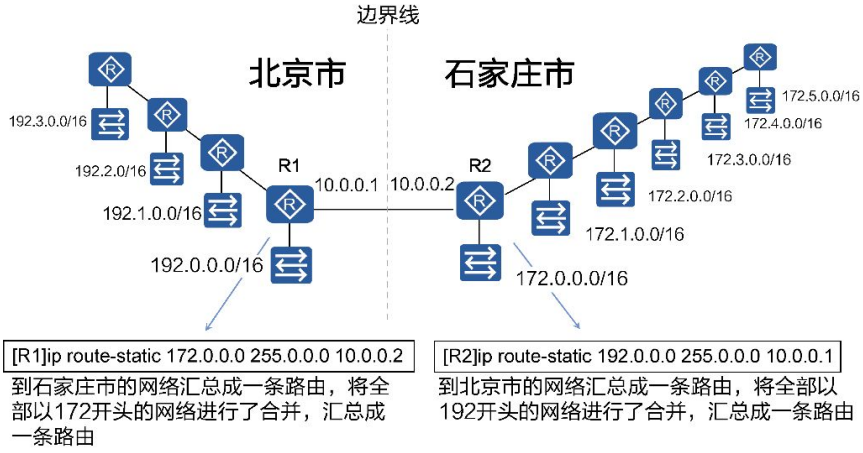


图5-10　路由汇总

可以看出规律，添加路由时，网络位越少（子网掩码中1的个数越少），路由汇总的网段越多。

5.2.2　路由汇总例外

如图5-11所示，在北京市有个网络使用了172.16.10.0/24网段，后来石家庄的网络连接北京市的网络，石家庄市的网络规划使用172.16打头的网段。在这种情况下，北京市网络的路由器还能不能把石家庄市的网络汇总成一条路由呢？

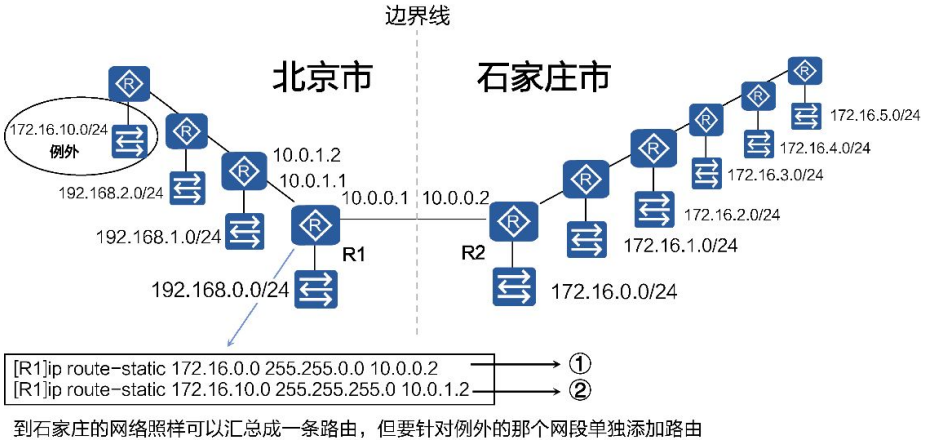


图5-11　路由汇总例外

在这种情况下，在北京市的路由器中照样可以把到石家庄市网络的路由汇总成一条路由，但要针对例外的网段单独再添加一条路由，如图5-10所示。

如果路由器R1收到目标地址是172.16.10.2的数据包，应该使用哪一条路由进行路径选择呢？

因为该数据包的目标地址与第①条路由和第②条路由都匹配，路由器将使用最精确匹配的那条路由来转发数据包，这叫作最长前缀匹配（Longest Prefix Match）。它是指在IP中被路由器用于在路由表中进行选择的一种算法。因为路由表中的每个表项都指定了一个网络，所以一个目的地址可能与多个表项匹配。最明确的一个表项（即子网掩码最长的一个）就叫作最长前缀匹配。之所以这样称呼它，是因为这个表项也是路由表中，与目的地址的高位匹配得最多的表项。

下面举例说明什么是最长前缀匹配算法，比如在路由器中添加了3条路由：

```
[R1]ip route-static 172.0.0.0  255.0.0.0  10.0.0.2            --
第1条路由
[R1]ip route-static 172.16.0.0  255.255.0.0  10.0.1.2          --
第2条路由
[R1]ip route-static 172.16.10.0  255.255.255.0  10.0.3.2       --
第3条路由
```

路由器R1收到一个目标地址是172.16.10.12的数据包，会使用第3条路由转发该数据包。路由器R1收到一个目标地址是172.16.7.12的数

据包，会使用第2条路由转发该数据包。路由器R1收到一个目标地址是172.18.17.12的数据包，会使用第1条路由转发该数据包。

路由表中常常包含一个默认路由。这个路由在所有表项都不匹配的时候有着最短的前缀匹配。本章5.3节讲解默认路由。

5.2.3 无类域间路由（CIDR）

为了让初学者容易理解，以上讲述的路由汇总通过将子网掩码向左移8位，合并了256个网段。无类域间路由（CIDR）采用13～27位可变网络ID，而不是A、B、C类网络ID所用的固定的8、16和24位。这样可以将子网掩码向左移动1位以合并两个网段；向左移动2位以合并4个网段；向左移动3位以合并8个网段；向左移动n位，就可以合并2^n个网段。

下面就举例说明CIDR如何灵活地对连续的子网进行精确合并。如图5-12所示，在A区有4个连续的C类网络，通过将子网掩码前移2位，可以将这4个C类网络合并到192.168.16.0/22网段。在B区有2个连续的子网，通过将子网掩码左移1位，可以将这两个网段合并到10.7.78.0/23网段。

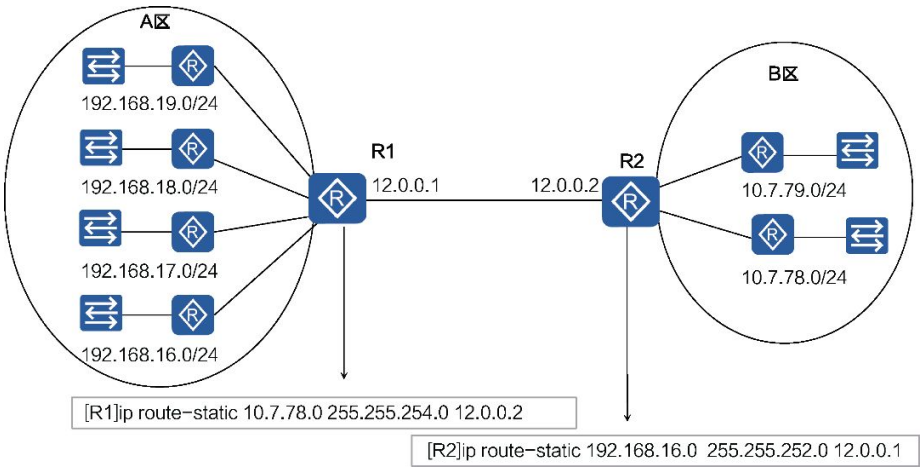


图5-12　使用CIDR简化路由表

学习本节知识时，一定要和第3章所讲的使用超网合并网段结合起来理解。

5.3 默认路由

默认路由是一种特殊的静态路由，指的是当路由表中没有与数据包的目的地址相匹配的路由时路由器能够做出的选择。如果没有默认路由，那么目的地址在路由表中没有匹配的路由的包将被丢弃。默认路由在某些时候非常有用，如连接末端网络的路由器，使用默认路由会大大简化路由器的路由表，减轻管理员的工作负担，提高网络性能。

5.3.1 全球最大的网段

在理解默认路由之前，先看看全球最大的网段在路由器中如何表示。在路由器中添加以下3条路由。

```
[R1]ip route-static 172.0.0.0  255.0.0.0  10.0.0.2              --
第1条路由
[R1]ip route-static 172.16.0.0  255.255.0.0  10.0.1.2           --
第2条路由
[R1]ip route-static 172.16.10.0  255.255.255.0  10.0.3.2        --
第3条路由
```

从上面3条路由可以看出，子网掩码越短（子网掩码写成二进制形式后1的个数越少），主机位越多，该网段的地址数量就越大。

如果想让一个网段包括全部的IP地址，就要求子网掩码短到极限，最短就是0，子网掩码变成了0.0.0.0，这也意味着该网段的32位二进制形式的IP地址都是主机位，任何一个地址都属于该网段。因

此，子网掩码为0.0.0.0的网段包括全球所有的IPv4地址，也就是全球最大的网段，换一种写法就是0.0.0.0/0。

在路由器中添加到0.0.0.0 0.0.0.0网段的路由，即默认路由。

```
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.0.2
--第4条路由
```

任何一个目标地址都与默认路由匹配，根据前面所讲的“最长前缀匹配”算法，可知默认路由是在路由器没有为数据包找到更为精确匹配的路由时最后匹配的一条路由。

下面的内容给大家讲解默认路由的几个经典应用场景。

5.3.2 使用默认路由作为指向Internet的路由

本案例是默认路由的一个应用场景。

某公司内网有A、B、C和D共4个路由器，有10.1.0.0/24、10.2.0.0/24、10.3.0.0/24、10.4.0.0/24、10.5.0.0/24、10.6.0.0/24共6个网段，网络拓扑和地址规划如图5-13所示。现在要求在这4个路由器中添加路由，使内网的6 个网段之间能够相互通信，同时这 6 个网段也要能够访问Internet。

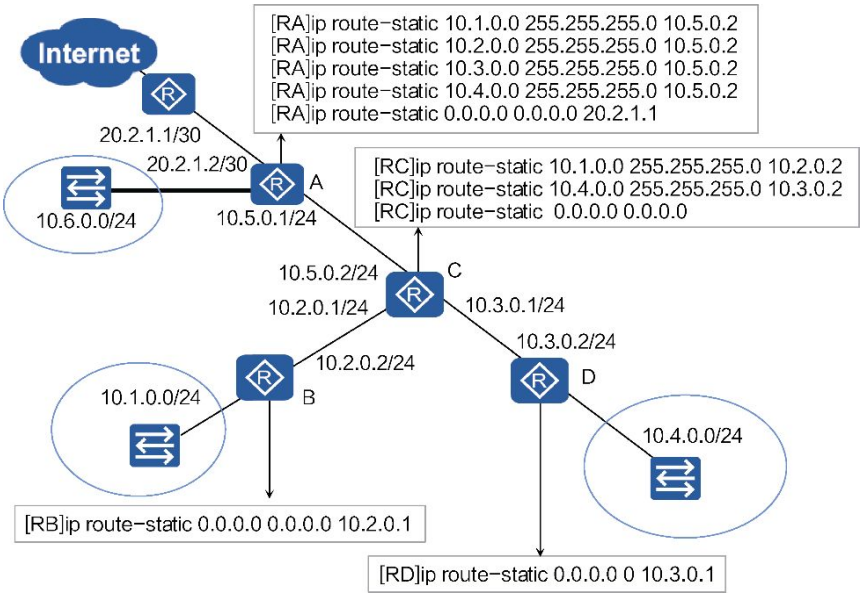


图5-13　使用默认路由简化路由表

路由器B和D是网络的末端路由器，直连两个网段，到其他网络都需要转发到路由器C，在这两个路由器中只需要添加一条默认路由即可。

对于路由器C来说，直连了3个网段，到10.1.0.0/24、10.4.0.0/24两个网段的路由需要单独添加，到Internet或10.6.0.0/24网段的数据包，都需要转发给路由器A，此时再添加一条默认路由即可。

对于路由器A来说，直连3个网段，对于没有直连的几个内网，需要单独添加路由，到Internet的访问只需要添加一条默认路由即可。

到Internet上所有网段的路由，只需要添加一条默认路由即可。

观察图5-13，看看A路由器中的路由表是否可以进一步简化。企业内网使用的网段可以合并到10.0.0.0/8网段中，因此在路由器A中，到内网网段的路由可以汇总成一条，如图5-14所示。大家想想路由器C中的路由表还能简化吗？

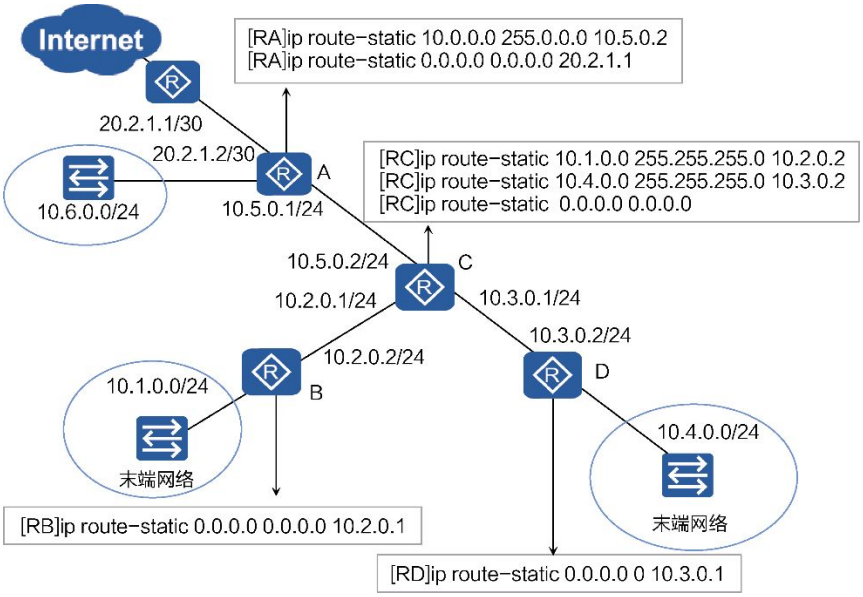


图5-14　路由器路由汇总和默认路由简化路由表

5.3.3　使用默认路由和路由汇总简化路由表

Internet是全球最大的互联网，也是全球拥有最多网段的网络。整个Internet上的计算机要想实现互相通信，就要正确配置Internet上路由器中的路由表。如果公网IP地址规划得当，就能够使用默认路由和路由汇总大大简化Internet上路由器中的路由表。

下面就举例说明Internet上的IP地址规划，以及网络中的各级路由器如何使用默认路由和路由汇总简化路由表。为了方便说明，在这

里只画出了3个国家。

国家级网络规划：英国使用30.0.0.0/8网段，美国使用20.0.0.0/8网段，中国使用40.0.0.0/8网段，一个国家分配一个大的网段，方便路由汇总。

中国国内的地址规划：对于省级IP地址规划，河北省使用40.2.0.0/16网段，河南省使用40.1.0.0/16网段，其他省份分别使用40.3.0.0/16、40.4.0.0/16、…、40.255.0.0/16网段。

河北省内的地址规划：石家庄地区使用40.2.1.0/24网段，秦皇岛地区使用40.2.2.0/24网段，保定地区使用40.2.3.0/24网段，如图5-15所示。

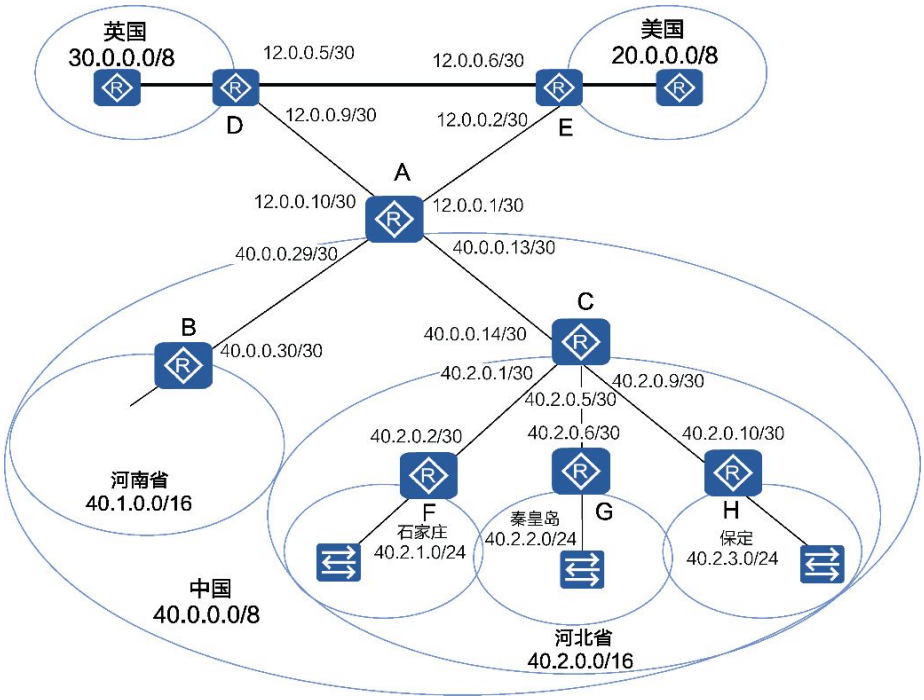


图5-15　Internet地址规划示意图

路由表的添加如图5-16所示，路由器A、D和E是中国、英国和美国的国际出口路由器。这一级别的路由器，到中国的只需要添加一条40.0.0.0 255.0.0.0路由，到美国的只需要添加一条20.0.0.0 255.0.0.0路由，到英国的只需要添加一条30.0.0.0 255.0.0.0路由。由于很好地规划了IP地址，所以可以将一个国家的网络汇总为一条路由，这一级路由器中的路由表就变得精简了。

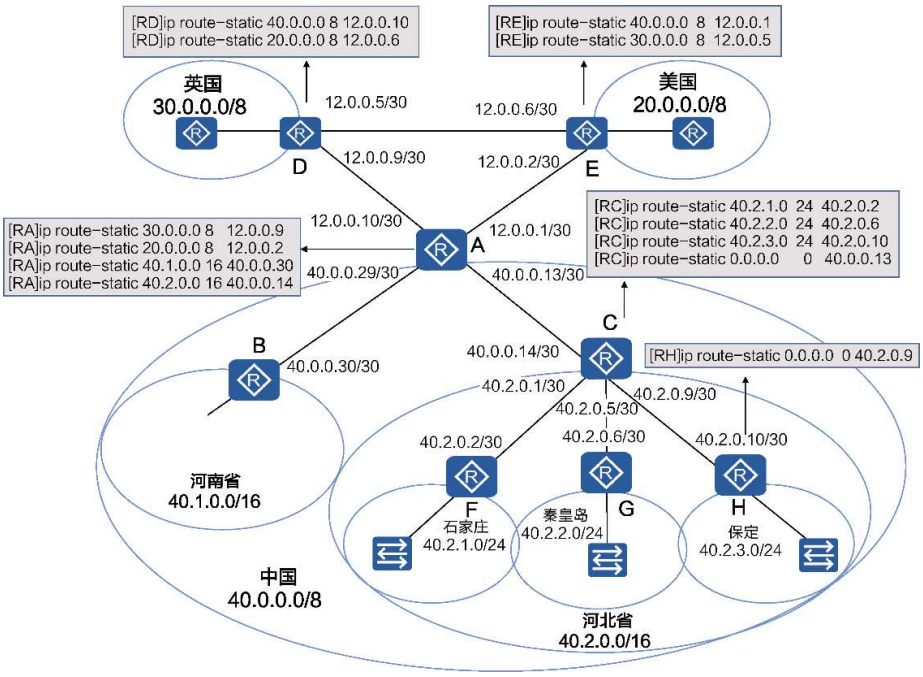


图5-16　使用路由汇总和默认路由简化路由表

中国的国际出口路由器A，除了添加到美国和英国两个国家的路由，还需要添加到河南省、河北省以及其他省份的路由。由于各个省份的IP地址也得到了很好的规划，所以一个省份的网络可以汇总成一条路由，这一级路由器的路由表也很精简。

对于河北省的路由器C，它的路由如何添加呢？对于路由器C来说，数据包除了到石家庄、秦皇岛和保定地区的网络以外，其他要么是出省的，要么是出国的，都需要转发到路由器A。在省级路由器C中要添加到石家庄、秦皇岛或保定地区的网络的路由，到其他网络的路由则使用一条默认路由指向路由器A。这一级路由器使用默认路由，也能够使路由表变得精简。

对于网络末端的路由器H、G和F来说，只需要添加一条默认路由指向省级路由器C即可。

总结：要想网络地址规划合理，骨干网上的路由器可以使用路由汇总精简路由表，网络末端的路由器可以使用默认路由精简路由表。

5.3.4　默认路由造成路由环路

如图5-17所示，网络中的路由器A、B、C、D、E、F连成一个环，要想让整个网络畅通，只需要在每个路由器中添加一条默认路由以指向下一个路由器的地址即可，配置方法如图5-17所示。

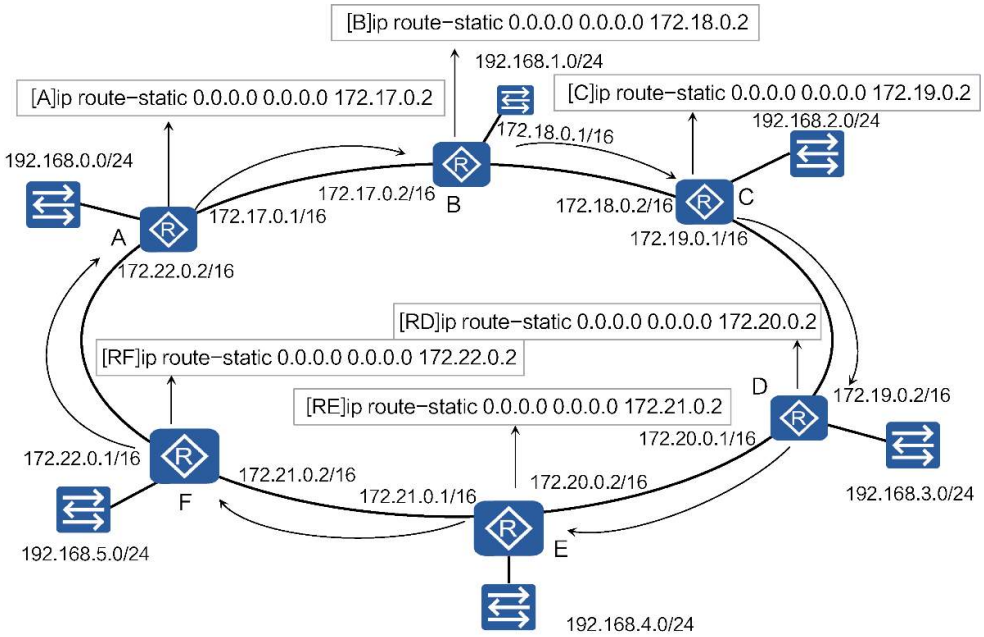


图5-17　环形网络使用默认路由

通过这种方式配置路由，网络中的数据包就沿着环路顺时针传递。下面就以网络中的计算机A和计算机B通信为例，如图5-18所示，计算机A到计算机B的数据包途经路由器F→A→B→　　C→D→E，计算机B到计算机A的数据包途经路由器E→F。如图5-18所示，可以看到数据包到达目标地址的路径和返回的路径不一定是同一条路径，数据包走哪条路径，完全由路由表决定。

该环状网络没有40.0.0.0/8这个网段，如果计算机A ping 40.0.0.2这个地址，会出现什么情况呢？分析一下。

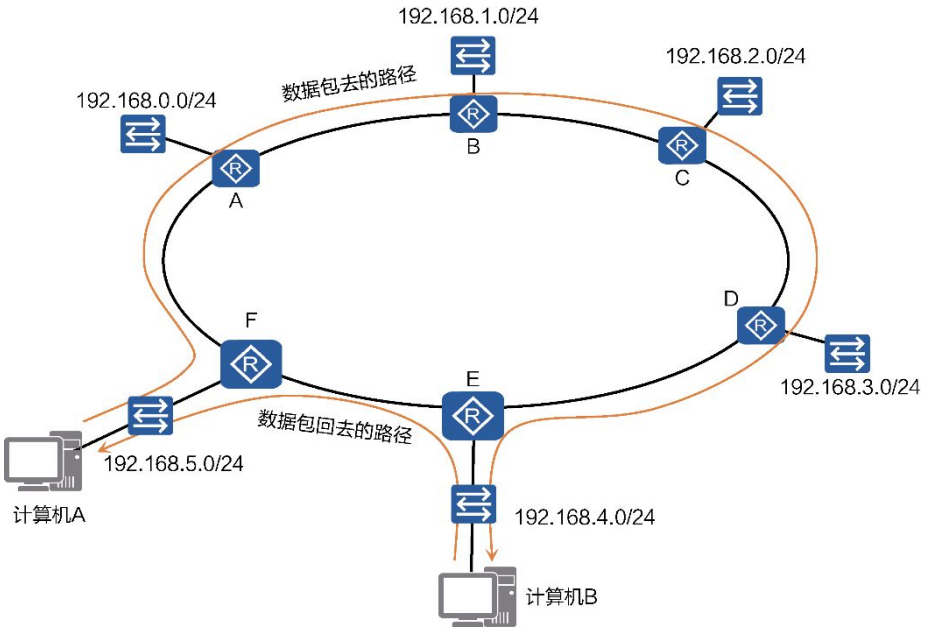


图5-18　数据包往返路径

如果计算机A ping 40.0.0.2这个地址，那么所有的路由器都会使用默认路由将数据包转发到下一个路由器。数据包会在这个环状网络中一直顺时针转发，永远也不能到达目标网络，并一直消耗网络带宽，这就形成一个路由环路。幸好数据包的网络层首部有一个字段用来指定数据包的生存时间，生存时间（time to live，TTL）是一个数值，TTL的作用是限制IP数据包在计算机网络中存在的时间。TTL的最大值是255，推荐值是64。

虽然TTL从字面上翻译，是指可以存活的时间，但实际上，TTL是IP数据包在计算机网络中可以经过的路由器的数量。TTL字段由IP数据包的发送者设置，在IP数据包从源地址到目标地址的整条转发路径上，每经过一个路由器，路由器都会修改TTL字段的值。具体的做法是把TTL的值减1，然后将IP数据包转发出去。如果在IP数据包到达目标

地址之前，TTL减少为0，路由器将会丢弃收到的TTL=0的IP数据包，并向IP数据包的发送者发送ICMP time exceeded消息。

上面讲到环状网络使用默认路由，造成数据包在环状网络中一直顺时针转发的情况。即便不是环状网络，使用默认路由也可能造成数据包在链路上往复转发，直到数据包的TTL耗尽。

如图5-19所示，网络中有3个网段、两个路由器。在RA路由器中添加默认路由，下一跳指向RB路由器；在RB路由器中也添加默认路由，下一跳指向RA路由器，从而实现这3个网段（172.16.0.0/24、172.17.0.0/24、172.18.0.0/24）间网络的畅通。

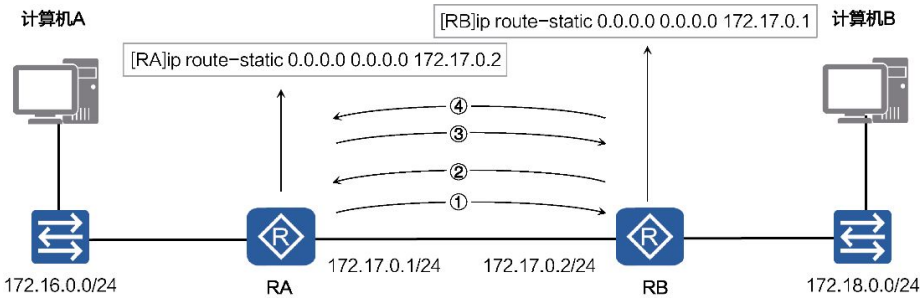


图5-19　默认路由产生的问题

该网络中没有40.0.0.0/8网段，如果计算机A ping 40.0.0.2这个地址，数据包会转发给RA，RA根据默认路由将该数据包转发给RB，RB使用默认路由将数据包转发给RA，RA再转发给RB，直到该数据包的TTL减为0。路由器丢弃该数据包，向发送者发送ICMP time exceeded消息。

5.3.5　让默认路由代替大多数网段的路由

在同一个网络中给路由器添加静态路由，不同的管理员可能会有不同的配置。总的原则是尽量使用默认路由和路由汇总让路由器上的路由表精简。

如图5-20所示，在路由器C上添加路由，有两种方案可以使网络畅通，第1种方案只需添加3条路由，第2种方案需要添加4条路由。

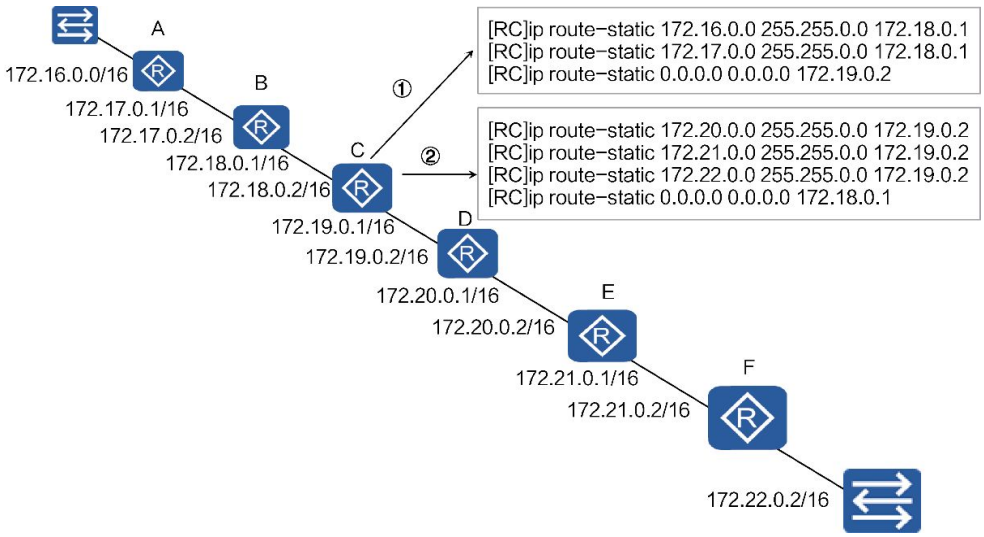


图5-20　默认路由代替大多数网络

让默认路由替代大多数网段的路由是明智的选择。在给路由器添加静态路由时，先要判断一下路由器哪边的网段多，针对这些网段使用一条默认路由，然后再针对其他网段添加路由。

5.3.6　Windows上的默认路由和网关

以上介绍了为路由器添加静态路由的方式。其实计算机也有路由表，可以在Windows操作系统上执行route print命令来显示Windows操

作系统上的路由表，执行netstat -r命令也可以实现相同的效果。

如图5-21所示，给计算机配置网关就是为计算机添加默认路由，网关通常是本网段路由器接口的地址。如果不配置网关，计算机将不能跨网段通信，因为不知道把到其他网段的下一跳给哪个接口。

如果计算机的本地连接没有配置网关，那么使用route add命令添加默认路由也可以。如图5-22所示，去掉本地连接的网关，在命令提示符下执行“netstat －r”将显示路由表，可以看到没有默认路由了。

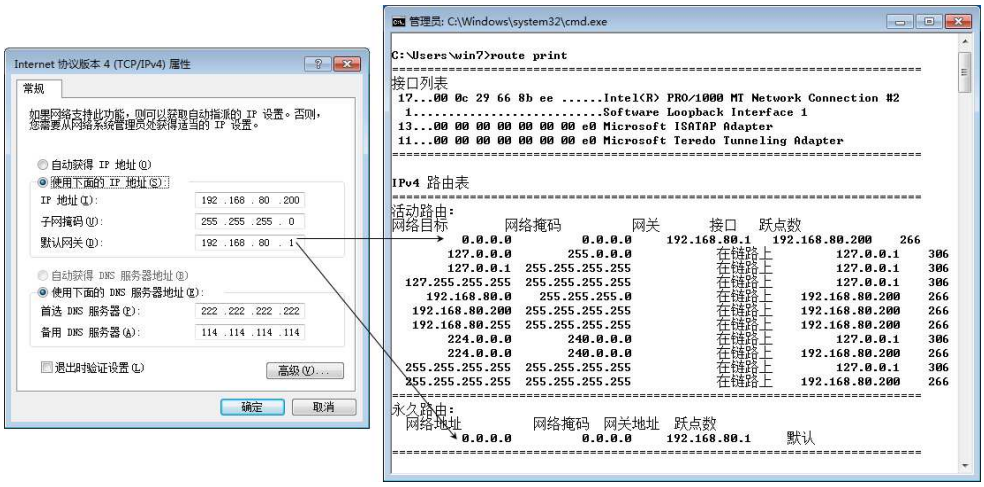


图5-21　网关等于默认路由

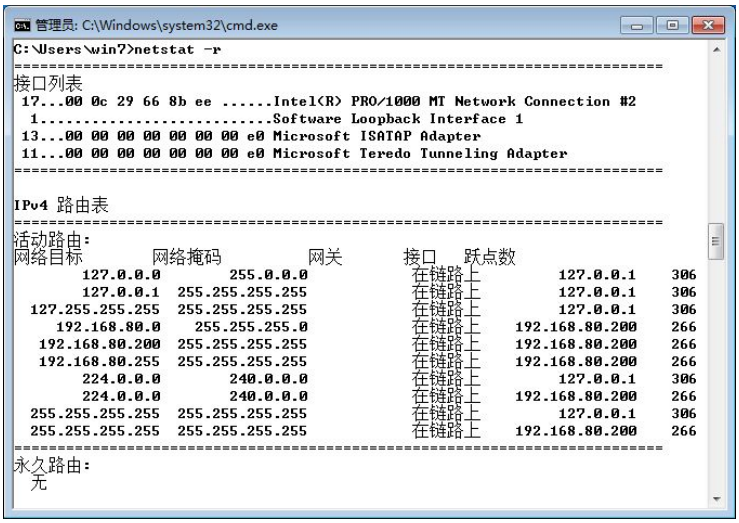


图5-22　查看路由表

在命令提示符下执行“route /?”可以看到该命令的帮助信息。

```
C:\Users\win7>route /?
```

操作网络路由表。

```
UTE [-f] [-p] [-4|-6] command [destination]
          [MASK netmask]  [gateway] [METRIC metric]  [IF interface]
-f        清除所有网关项的路由表。如果与某个命令结合使用，在运行该命令前，应清除路由表。
-p        与 ADD 命令结合使用时，将路由设置为在系统引导期间保持不变。默认情况下，重新启动系统时不保存路由。忽略所有其他命令，这始终会影响相应的永久路由。
Windows 95不支持此选项。
-4        强制使用 IPv4。
-6        强制使用 IPv6。

command         其中之一:
       PRINT    打印路由
       ADD      添加路由
       DELETE   删除路由
       CHANGE   修改现有路由
destination     指定主机。
MASK            指定下一个参数为"子网掩码"值。
netmask         指定此路由项的子网掩码值。如果未指定，默认设置为
255.255.255.255。
```

gateway	指定网关。
interface	指定路由的接口号码。
METRIC	指定跃点数，例如目标的成本。

如图5-23所示，输入route add 0.0.0.0 mask 0.0.0.0 192.168.80.1 -p，-p参数代表添加一条永久默认路由，即重启计算机后该默认路由依然存在。

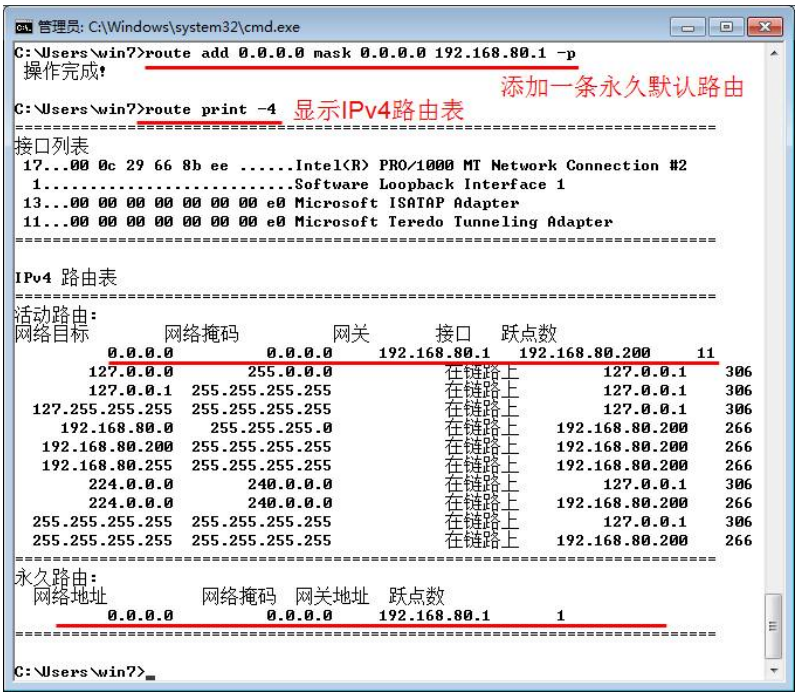


图5-23　添加默认路由

什么情况下会给计算机添加路由呢？下面介绍一个应用场景。

如图5-24所示，某公司在电信机房部署了一个Web服务器，该Web服务器需要访问数据库服务器。安全起见，将数据库单独部署到一个网段（内网）。该公司在电信机房又部署了一个路由器和一个交换机，并将数据库服务器部署在内网。

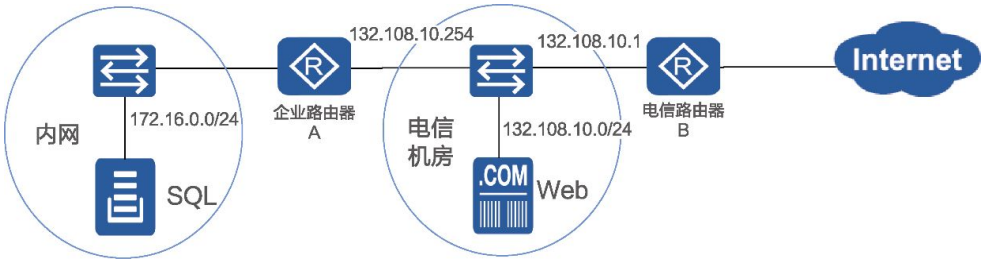


图5-24　需要添加静态路由

企业路由器没有添加任何路由，电信路由器也没有添加到内网的路由（关键是电信机房的网络管理员也不同意添加到内网的路由）。

在这种情况下，需要在Web服务器上添加一条到Internet的默认路由，再添加一条到内网的路由，如图5-25所示。

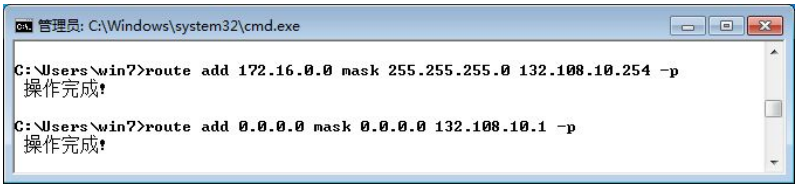


图5-25　添加路由

这种情况下千万别在Web服务器上添加两条默认路由（一条指向132.108.10.1，另一条指向132.108.10.254），或在本地连接中添加两个默认网关。如果添加两条默认路由，就相当于到Internet有两条等价路径，到Internet的一半流量将被发送到企业路由器，被企业路由器丢掉。

如果想删除到172.16.0.0 255.255.255.0网段的路由，执行以下命令：

```
route delete 172.16.0.0 mask 255.255.255.0
```

5.4　网络排错案例

前面给大家讲了网络畅通的条件，如何使用路由汇总和默认路由来简化路由表，以及如何管理Windows操作系统的路由表。道理虽然简单，但是应用到实际环境解决问题时却需要你真正理解并能够灵活应用。下面给大家讲解几个案例，希望能起到抛砖引玉、举一反三的作用。

5.4.1　站在全局的高度排除网络故障

石家庄车辆厂（中车石家庄公司）和唐山车辆厂（中车唐山公司）使用电信的专线连接。这两个公司都有自己的信息部门，肖工负责石家庄车辆厂的网络，张工负责唐山车辆厂的网络。

有一天石家庄车辆厂的肖工打来电话，说他在网络中新增加了一个网段：192.168.10.0/24，该网段不能访问唐山车辆厂的网络，如图5-26所示，让我帮忙分析一下。

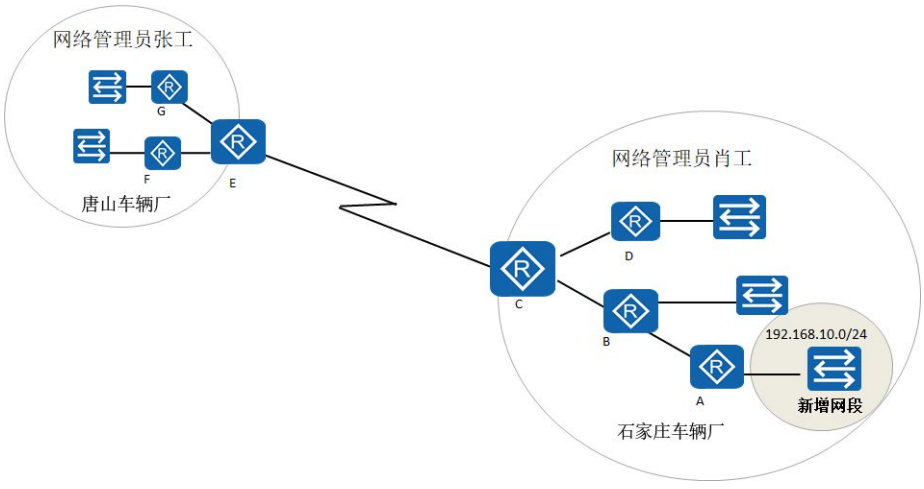


图5-26　企业网络

我首先想到的是路由问题，我问他是否在网络中的路由器上添加了到新增网段的路由，他回答“添加了”，新增网段中的计算机能够访问石家庄车辆厂的任何网段，就是不能访问唐山车辆厂的网络。

然后我就根据网络畅通的条件（数据包能去能回）来分析，新增的网段中的计算机发送的数据包是否能够到达唐山车辆厂的网络。让肖工检查石家庄车辆厂的路由器A、B、C、D，查看这些路由器的路由表，查看是否有到唐山车辆厂网络的路由。发现有到唐山车辆厂网络的路由，这就保证石家庄车辆厂发送的数据包能够到唐山车辆厂的网络（能去）。

下面该检查数据包是否能回了，让肖工检查唐山车辆厂的路由器是否有到达新增网段的路由，肖工说：“唐山车辆厂的网络不归我管，要想添加路由需要联系张工。”可见问题就出在这儿！

唐山车辆厂网络中的路由器没有到新增网段的路由，新增网段的计算机给唐山车辆厂发送数据包将有去无回。周一上班，肖工联系了唐山车辆厂的网络管理员张工，添加了到新增网段的路由，网络畅通。

从本案例来说，网络不通除了检查你所管辖的网络中路由器是否配置了正确的路由，还要检查远端网络的路由器是否配置了正确的路由。

5.4.2　计算机网关也很重要

某医院信息中心张主任，有一天给我打电话说他们的计算机不能访问服务器，上百度查了很多文章也没搞定，让我帮忙分析一下。我让他给我画了一张网络拓扑的草图，如图5-27所示。

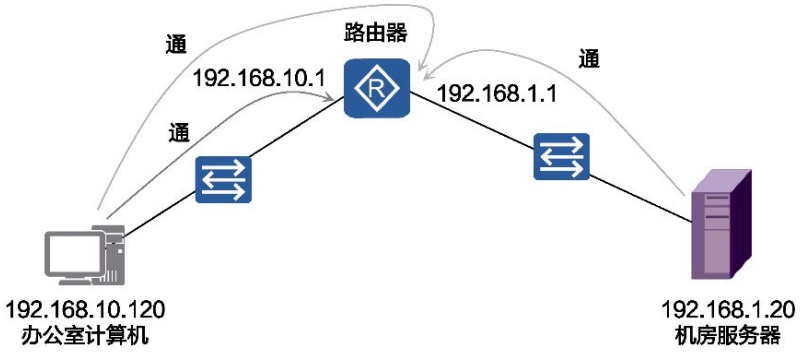


图5-27　服务器没有设置网关

网络很简单，路由器连接两个网段，办公室的计算机不能访问机房的服务器，在办公室的计算机上ping 192.168.1.20，请求超时。

来看网络拓扑，路由器直接连接两个网段，根本不需要添加路由，这个网络就应该能畅通。

电话里我让张主任按照我说的步骤排错，并告诉我测试结果，过程如下。

（1）先检查办公室计算机和机房服务器的网线连接是否正常，IP地址是否正确，查看IP地址的命令是ipconfig /all。网线连接正常，办公室计算机和机房服务器IP地址正确。

（2）在办公室计算机上ping 192.168.10.1，先测试一下是否和网关能通，测试结果“通”。

（3）再在办公室计算机上ping 192.168.1.1，测试结果“通”，说明办公室的计算机能够访问服务器网段。

（4）然后在机房服务器上ping 192.168.1.1，测试一下是否和服务器的网关能通，测试结果“通”。

我只好怀疑是不是机房服务器启用了防火墙，让张主任关闭机房服务器的防火墙，结果办公室的计算机还是不能ping通机房服务器。

这就百思不得其解了，能想到的原因都检查了还是找不到原因，只能去现场解决问题了。去现场后，第一件事情就是检查计算机的网络设置，输入“ipconfig /all”查看IP地址、子网掩码和网关，结果发现服务器没有设置网关，只是设置了IP地址和子网掩码。电话里我只是让张主任检查IP地址是否正确，忘了说也要检查网关。

服务器不设置网关，办公室计算机ping 192.168.1.20数据包是能够到达服务器的，但服务器返回响应数据包却不知道下一跳应该给哪个接口。这就是数据包有去无回造成的网络故障。

总结：我们排除网络故障，除了检查沿途路由器的路由表，还要检查相互通信的计算机是否设置了正确的网关。

5.5 习题

1. 华为路由器静态路由的配置命令为（　　）。

A. ip route-static

B. ip route static

C. route-static ip

D. route static ip

2. 假设有下面4条路由：170.18.129.0/24、170.18.130.0/24、170.18.132.0/24和170.18.133.0/24。如果进行路由汇总，能覆盖这4条路由的地址是（　　）。

A. 170.18.128.0/21

B. 170.18.128.0/22

C. 170.18.130.0/22

D. 170.18.132.0/23

3. 假设有两条路由21.1.193.0/24和21.1.194.0/24，如果进行路由汇总，覆盖这两条路由的地址是（　　）。

A. 21.1.200.0/22

B. 21.1.192.0/23

C. 21.1.192.0/22

D. 21.1.224.0/20

4. 路由器收到一个IP数据包，其目标地址为202.31.17.4，与该地址匹配的子网是（　　）。

A. 202.31.0.0/21

B. 202.31.16.0/20

C. 202.31.8.0/22

D. 202.31.20.0/22

5. 假设有两个子网210.103.133.0/24和210.103.130.0/24，如果进行路由汇总，得到的网络地址是（　　）。

A. 210.103.128.0/21

B. 210.103.128.0/22

C. 210.103.130.0/22

D. 210.103.132.0/20

6．在路由表中设置一条默认路由，目标地址和子网掩码应为（　　）。

A．127.0.0.0　255.0.0.0

B．127.0.0.1　0.0.0.0

C．1.0.0.0　255.255.255.255

D．0.0.0.0　0.0.0.0

7．网络122.21.136.0/24和122.21.143.0/24经过路由汇总后，得到的网络地址是（　　）。

A．122.21.136.0/22

B．122.21.136.0/21

C．122.21.143.0/22

D．122.21.128.0/24

8．路由器收到一个数据包，其目标地址为195.26.17.4，该地址属于（　　）子网。

A．195.26.0.0/21

B．195.26.16.0/20

C. 195.26.8.0/22

D. 195.26.20.0/22

9. 如图5-28所示，R1路由器连接的网段在R2路由器上汇总成一条路由192.1.144.0/20，（　　）数据包会被R2路由器使用这条汇总的路由转发给R1。

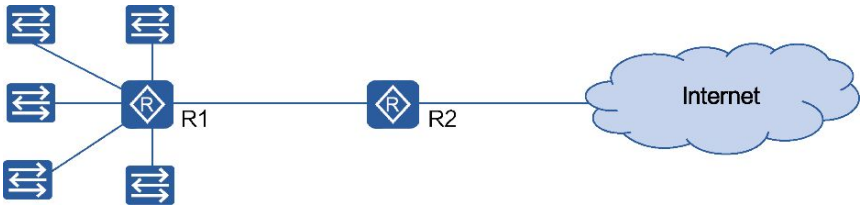


图5-28　示例网络（一）

A. 192.1.159.2

B. 192.1.160.11

C. 192.1.138.41

D. 192.1.1.144

10. 如图5-29所示，需要在RouterA和RouterB路由器中添加路由表，让A网段和B网段能够相互访问。

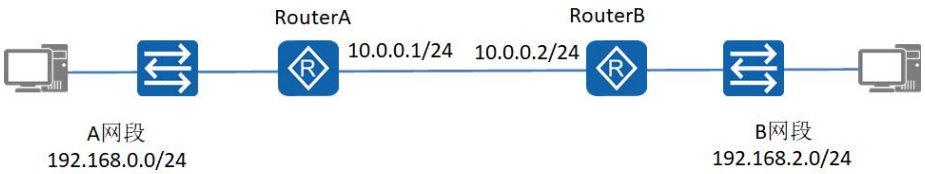


图5-29　示例网络（二）

[RouterA]ip route-

static _____ _____ _____

[RouterB]ip route-

static _____ _____ _____

11. 如图5-30所示，要求192.168.1.0/24网段到达192.168.2.0/24网段的数据包，经过R1R2R4；192.168.2.0/24网段到达192.168.1.0/24网段的数据包，经过R4R3R1。在这4个路由器上添加静态路由，让192.168.1.0/24和192.168.2.0/24两个网段能够相互通信。

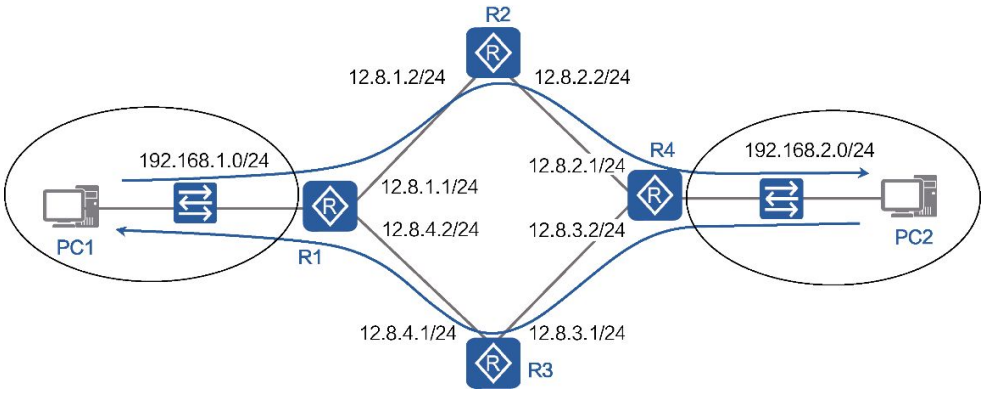


图5-30　示例网络（三）

[R1]ip route-

static _____ _____ _____

[R2]ip route-

static _____ _____ _____

[R3]ip route-

static _____ _____ _____[R4]ip

route-static _____ _____ _____

12. 在路由器上执行以下命令来添加静态路由。

[R1]ip route-static 0.0.0.0 0 192.168.1.1

[R1]ip route-static 10.1.0.0 255.255.0.0 192.168.3.3

[R1]ip route-static 10.1.0.0 255.255.255.0 192.168.2.2

连线图5-31左侧的目标IP地址和右侧路由器的下一跳地址。

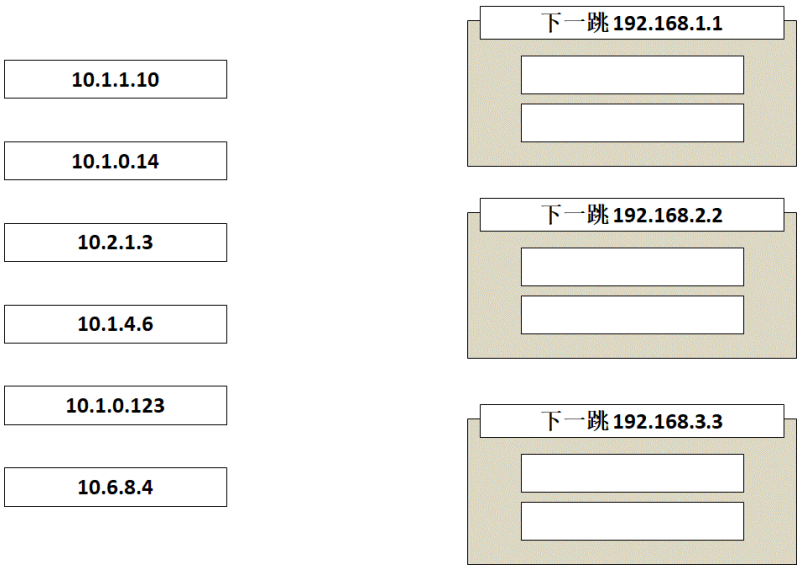


图5-31　连线目标IP地址和下一跳地址

13. 下列静态路由配置中正确的是（　　）。

A. [R1]ip route-static 129.1.4.0 16 serial 0

B. [R1]ip route-static 10.0.0.2 16 129.1.0.0

C. [R1]ip route-static 129.1.0.0 16 10.0.0.2

D. [R1]ip route-static 129.1.2.0 255.255.0.0 10.0.0.2

14. IP报文头部有一个TTL字段，以下关于该字段的说法中正确的是（　　）。

A. 该字段长度为7位

B. 该字段用于数据包分片

C. 该字段用于数据包防环

D. 该字段用来表述数据包的优先级

15. 路由器在转发某个数据包时，如果未匹配到对应的明细路由且无默认路由，将直接丢弃该数据包，正确与否？（　　）。

A. 正确

B. 错误

16. 以下哪一项不包含在路由表中？（　　）

A. 源地址

B. 下一跳

C．目标网络

D．路由开销

17．下列关于华为设备中静态路由的优先级说法中，错误的是（　　）。

A．静态路由器优先级值的范围为0～65535

B．静态路由器优先级的默认值为60

C．静态路由的优先级值可以指定

D．静态路由的优先级值为255表示该路由不可用

18．下面关于IP报文头部中TTL字段的说法中，正确的是（　　）。

A．TTL定义了源主机可以发送的数据包数量

B．TTL定义了源主机可以发送数据包的时间间隔

C．IP报文每经过一台路由器时，其TTL值会被减一

D．IP报文每经过一台路由器时，其TTL值会被加一

19．对于命令ip route-static 10.0.12.0 255.255.255.0 192.168.11，以下描述中正确的是（　　）。

A．此命令配置一条到达192.168.1.1网络的路由

B．此命令配置一条到达10.0.12.0/24网络的路由

C．该路由的优先级为100

D．如果路由器通过其他协议学习到和此路由相同的网络的路由，路由器将会优先选择此路由

20．已知某台路由器的路由表中有如下两个条目：

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
9.0.0.0/8	OSPF	10	50	1.1.1.1	Serial0
9.1.0.0/16	RIP	100	5	2.2.2.2	Ethernet0

如果该路由器要转发目标地址为9.1.4.5的报文，则下列说法中正确的是（　　）。

A．选择第一项作为最优匹配项，因为OSPF协议的优先级较高

B．选择第二项作为最优匹配项，因为RIP的开销较小

C．选择第二项作为最优匹配项，因为出口是Ethternet0，比Serial 0速度快

D．选择第二项作为最优匹配项，因为该路由项对于目标地址9.1.4.5来说，是更为精确的匹配

21．下面哪个程序或命令可以用来探测从源节点到目标节点数据报文所经过的路径？（　　）

A. route

B. netstat

C. tracert

D. send

22. 如图5-32所示，和总公司网络连接的网络是分公司的内网。分公司为了访问Internet，又组建了公司外网，分公司内网和外网的地址规划如图5-31所示。分公司计算机有两根网线，访问Internet时接分公司外网，访问总公司网络时接分公司内网。现在需要规划一下分公司的网络，在不用切换网络的情况下，让分公司计算机既能访问Internet，又能访问总公司网络。

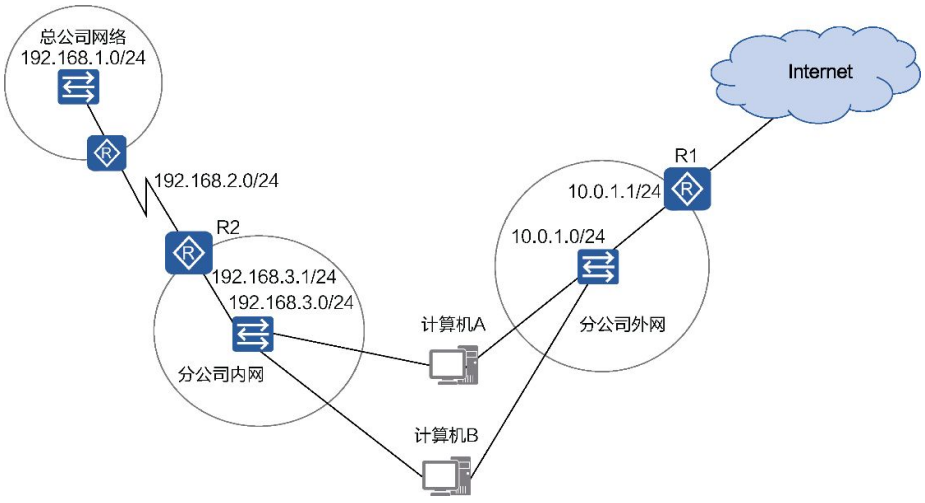


图5-32　总公司网络和分公司网络

第6章　动态路由

本章内容

- 什么是动态路由
- 动态路由——OSPF协议
- 配置OSPF协议

静态路由不能随着网络的变化自动调整，且在大规模网络中，人工管理路由器的路由表是一件非常艰巨的任务且容易出错。本章讲解动态路由OSPF协议，让路由器使用动态路由协议自动构建路由表。

本章讲解OSPF协议的工作过程，OSPF协议选择最佳路径的标准，将网络中的路由器配置为使用OSPF协议构建路由表，查看OSPF协议邻居表、路由表、链路状态表。

6.1　什么是动态路由

第5章介绍了在路由器上通过ip route-static添加的路由是静态路由。如果网络有变化，比如增加一个网段，就需要为网络中的所有没有直连的路由器添加到新网段的路由。如果某个网段更改成新的网段，就需要在网络中的路由器上删除到原来网段的路由，并添加到新网段的路由。如果网络中的某条链路断了，静态路由依然会把数据包转发到该链路，这就造成了网络不通。

总之，静态路由不能随着网络的变化自动调整路由器的路由表。在网络规模比较大的情况下，人工添加路由也是一件很麻烦的事情。下面要讲的动态路由能够让路由器自动学习构建路由表，并根据链路的状态动态寻找到各个网段的最佳路径。

动态路由就是配置网络中的路由器以运行动态路由协议。路由表项是通过相互连接的路由器之间交换彼此信息、然后按照一定的算法计算出来的，而这些路由信息是周期性更新的，以适应不断变化的网络，并及时获得最优的寻径效果。

动态路由协议有以下功能。

- 知道有哪些邻居路由器。
- 学习到网络中有哪些网段。
- 学习到某个网段的所有路径。
- 从众多的路径中选择最佳的路径。
- 维护和更新路由信息。

下面来学习动态路由协议，也就是配置路由器使用动态路由协议RIP和OSPF来构造路由表。

6.2　动态路由——OSPF协议

下面学习能够在Internet上使用的动态路由协议——OSPF协议。

OSPF（Open Shortest Path First）协议是开放式最短路径优先协议，该协议是链路状态协议。OSPF协议通过路由器之间通告链路的状态来建立链路状态数据库。网络中所有的路由器具有相同的链路状态数据库，通过链路状态数据库就能构建出网络拓扑（即哪个路由器连接哪个路由器，以及连接的开销，带宽越高开销越低）。运行OSPF协议的路由器通过网络拓扑计算到各个网络的最短路径（即开销最小的路径），路由器使用这些最短路径来构造路由表。

6.2.1　OSPF协议简介

OSPF协议是一种典型的链路状态（link-state）路由协议。运行OSPF协议的路由器（OSPF路由器）之间交互的是链路状态（Link State，LS）信息，而不是直接交互路由。OSPF路由器将网络中的链路状态信息收集起来，存储在链路状态数据库（LSDB）中。网络中的路由器都有相同的链路状态数据库，也就是相同的网络拓扑结构。每台OSPF路由器都采用最短路径优先（SPF）算法计算到达各个网段的最短路径，并将这些最短路径形成的路由加载到路由表中。

OSPF协议主要有以下优点。

（1）OSPF支持可变长子网掩码（Variable Length Subnet Mask，VLSM）和手动路由汇总。

（2）OSPF协议能够避免路由环路。每个路由器通过链路状态数据库使用最短路径的算法，这样不会产生环路。

（3）OSPF收敛速度快，能够在最短的时间内将路由变化传递到整个自治系统。

（4）OSPF适合大范围的网络。OSPF协议对于路由的跳数是没有限制的。多区域的设计使得OSPF能够支持更大规模的网络。

（5）以开销作为度量值。OSPF协议在设计时，就考虑到了链路带宽对路由度量值的影响。OSPF协议以开销值为标准，而链路开销和链路带宽，正好形成了反比的关系，带宽越高，开销就会越小，这样一来，OSPF选路主要基于带宽因素。

6.2.2　由最短路径生成路由表

运行OSPF协议的路由器，根据链路状态数据库就能生成一个完整的网络拓扑，所有的路由器都有相同的网络拓扑。如图6-1所示，它标出了路由器连接的网段和每条链路上由带宽计算出来的开销。为了便于计算，标出的开销值都比较小。为了描述简练，路由器之间的连接占用的网段在这里没有画出，也不参与下面的讨论。

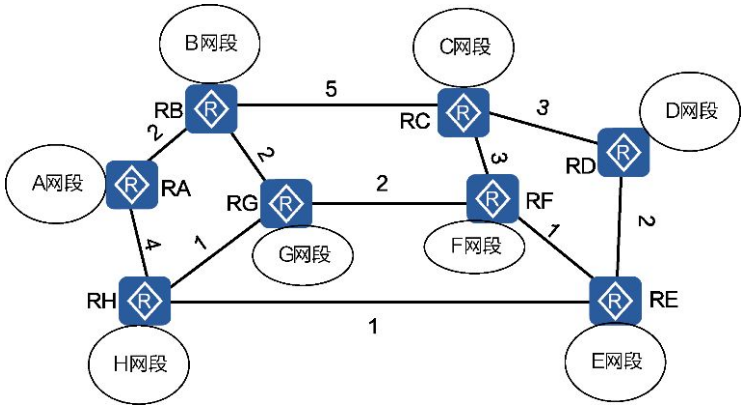


图6-1　链路状态生成的网络拓扑

每个路由器都利用最短路径优先算法计算出以自己为根的、无环路的、拥有最短路径的一棵树。在这里不阐述最短路径算法的过程，只展现结果。图6-2展示了RA路由器的最短路径树，即到其他网段累计开销最低的线路，该路线是无环路的。

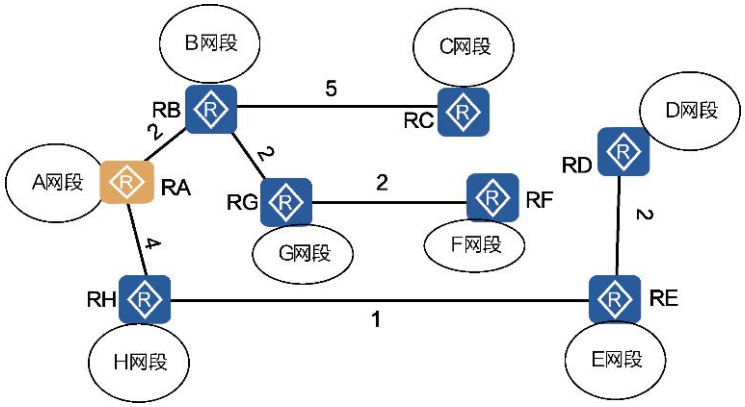


图6-2　RA路由器计算的最短路径

由图6-2可知从RA路由器到网段的最小累计开销，具体如下所示。

到B网段：RA→RB，累计开销2。

到C网段：RA→RB→RC，累计开销7。

到D网段：RA→RH→RE→RD，合计7。

到E网段：RA→RH→RE，合计5。

到F网段：RA→RB→RG→RF，合计6。

到G网段：RA→RB→RG，合计4。

到H网段：RA→RH，合计4。

图6-3展示了RH路由器的最短路径树，即到其他网段累计开销最低的路径，该路径也是无环路的。

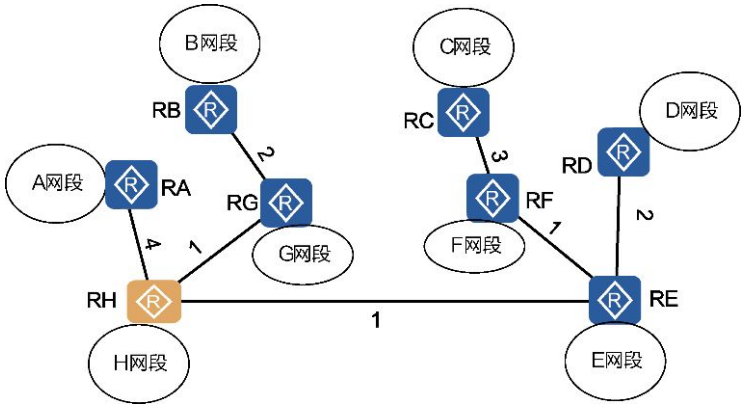


图6-3　RH路由器计算的最短路径

为了快速为数据包选择转发路径，每个路由器还要根据计算的最短路径树生成到各个网段的路由。如图6-4所示，展示了RA路由器根据最短路径生成的路由。

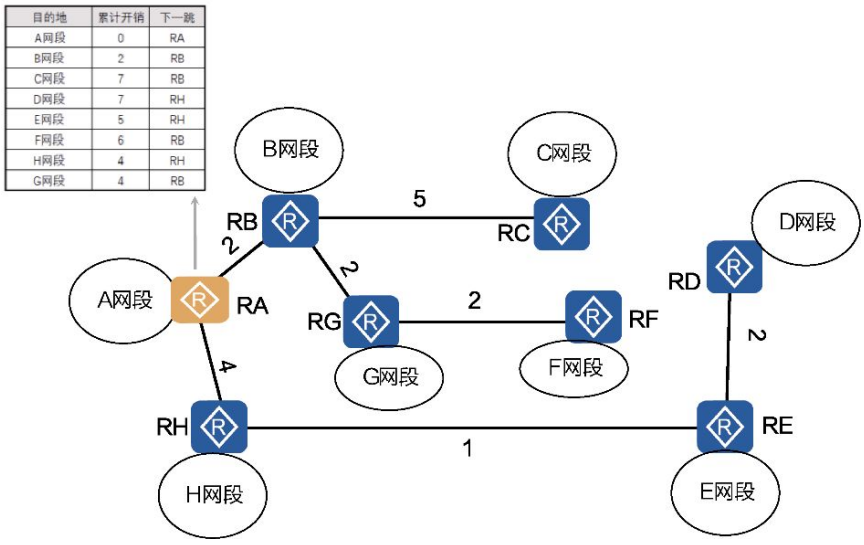


图6-4　生成路由表

6.2.3　OSPF协议相关术语

（1）Router-ID。

网络中运行OSPF协议的路由器都要有一个唯一的标识——Router-ID。Router-ID在网络中不可以重复，否则路由器收到的链路状态就无法确定发起者的身份。OSPF路由器发出的链路状态都有自己的Router-ID。Router-ID使用IP地址的形式表示，确定Router-ID的方法有以下几种。

- 手动指定Router-ID。
- 选择路由器上环回接口中最大的IP地址，也就是数字最大的IP地址，例如，C类地址优先于B类地址，一个非活动接口的IP地址是不能用作Router-ID的。
- 如果没有活动的Loopback接口，则选择活动物理接口中最大的IP地址。

在实际项目中，通常会通过手动配置的方式为设备指定Router-ID。通常的做法是将Route-ID配置为与该设备某个接口（通常为Loopback接口）的IP地址一致的值。

（2）度量值。

OSPF使用Cost（开销）作为路由的度量值。每个激活了OSPF的接口都会维护一个接口Cost值，默认接口Cost 值 $= \dfrac{100\text{Mbit/s}}{\text{接口带宽}}$。其中100Mbit/s为OSPF指定的默认参考值，该值是可配置的。

从公式可以看出，OSPF协议选择最佳路径的标准是带宽，带宽越高，计算出来的开销越低。到达目标网络的各条链路中累计开销最低的就是最佳路径。

例如一个带宽为 10Mbit/s 的接口，计算开销的方法为：将 10Mbit 换算成 bit，为10000000bit，然后用 100000000 除以该带宽，结果为100000000/10000000 = 10，所以一个10Mbit/s的接口，OSPF认为该接口的度量值为10。需要注意的是，在计算中，带宽的单位取bit/s而不是kbit/s，例如一

个带宽为100Mbit/s的接口，开销值为100000000/100000000=1，因为开销值必须为整数，所以即使是一个带宽为1000Mbit/s（1Gbit/s）的接口，开销值也和100Mbit/s一样，为1。如果路由器要经过两个接口才能到达目标网络，那么很显然，两个接口的开销值要累加起来，才算是到达目标网络的度量值。所以OSPF路由器计算到达目标网络的度量值时，必须要将沿途所有接口的开销值累加起来，在累加时，只计算出接口，不计算进接口。如图6-5所示，它展示了接口开销和累计开销。

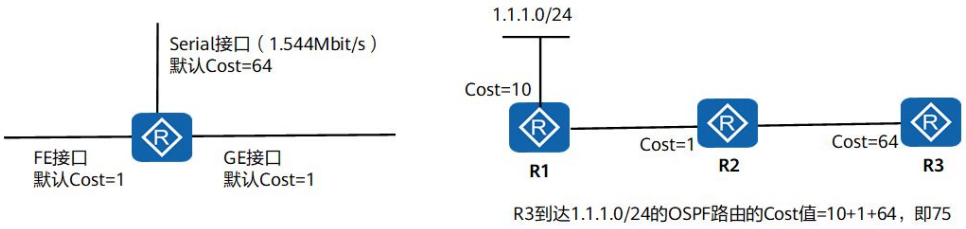


图6-5　接口开销和累计开销

OSPF会自动计算接口上的开销值，但也可以手动指定接口的开销值，手动指定的优先于自动计算的。

（3）链路（Link）。

链路是路由器上的接口，这里指运行在OSPF进程下的接口。

（4）链路状态（link-state）。

链路状态就是OSPF接口的描述信息，例如接口的IP地址、子网掩码、网络类型、开销值等。OSPF路由器之间交换的并不是路由表，而是链路状态。

（5）邻居（Neighbor）。

同一个网段上的路由器可以成为邻居。通过Hello报文发现邻居，Hello 报文使用IP多播方式在每个端口定期发送。路由器一旦在其相邻路由器的Hello

报文中发现自己，则它们就成为邻居关系了。在这种方式中，需要通信的双方确认。

（6）邻接状态。

邻接状态是相邻路由器交互数据库描述、链路状态请求、链路状态更新、链路状态确认报文完成后，两端设备的链路状态数据库完全相同，从而进入邻接状态。

6.2.4 OSPF工作过程

运行OSPF协议的路由器有3张表，分别是邻居表、链路状态表（链路状态数据库）和路由表。下面以这3张表的产生过程为基础，分析在这个过程中路由器发生了哪些变化，从而说明OSPF协议的工作过程。

（1）生成邻居表。

OSPF区域的路由器首先要跟邻居路由器建立邻接关系。当一个路由器刚开始工作时，每隔10s就发送一个Hello数据包，它通过发送Hello数据包得知它有哪些相邻的路由器在工作，以及将数据发往相邻路由器所付出的“代价”，然后生成“邻居表”。

若40s后没有收到某个相邻路由器发来的Hello数据包，则可认为该相邻路由器是不可到达的，路由器会立即修改链路状态数据库，并重新计算路由表。

图6-6展示了R1和R2路由器通过Hello数据包建立邻居表的过程。一开始R1路由器接口的OSPF状态为down state，R1路由器发送一个Hello数据包之后，状态变为init state，等收到R2路由器发过来的Hello数据包，看到自己的Router-ID出现在其他路由器应答的邻居表中，这就建立了邻居关系，并将状态更改为two-way state。

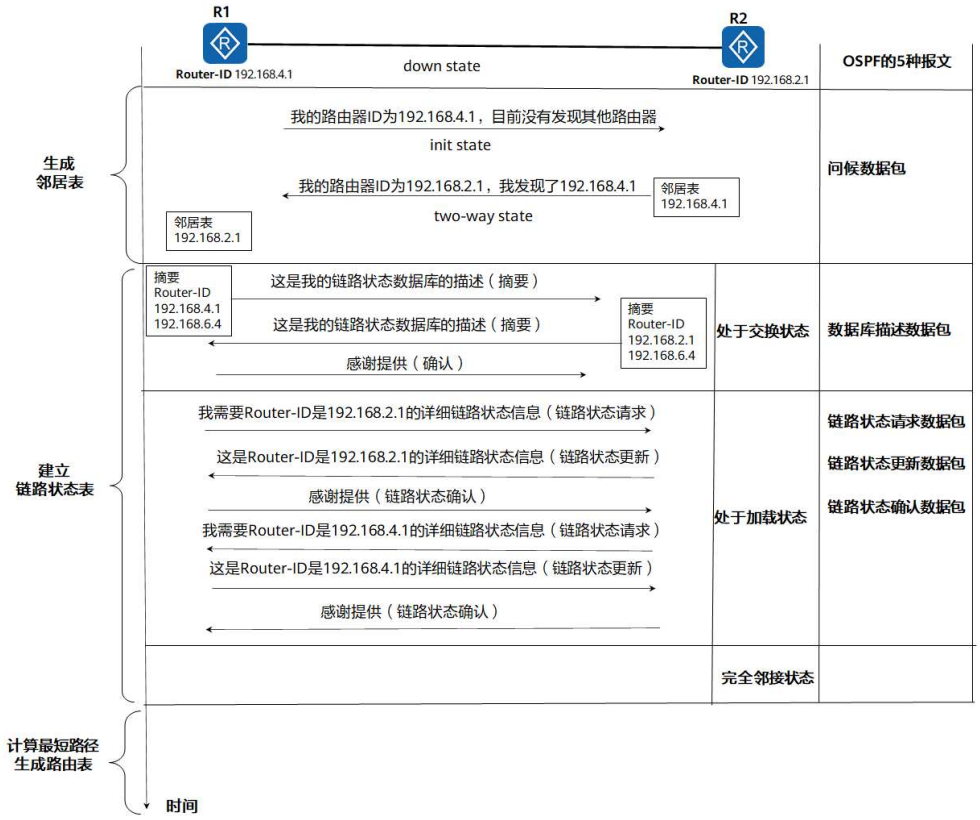


图6-6　OSPF协议的工作过程

（2）建立链路状态表。

如图6-6所示，建立邻居表之后，相邻路由器就要交换链路状态建立链路状态表。在建立链路状态表的时候，路由器要经历交换状态、加载状态、完全邻接状态。

交换状态：OSPF让每一个路由器用数据库描述数据包和相邻路由器交换本数据库中已有的链路状态摘要（描述）信息。发送的摘要信息包含自己链路状态表中所有的路由器（Router-ID）。

加载状态：经过与相邻路由器交换数据库描述数据包后，路由器就使用链路状态请求数据包，向对方请求自己所缺少的某些路由器相关的链路状态的详

细信息。通过这一系列的分组交换，全网同步的链路状态数据库（Link State DataBase，LSDB）就建立了。

完全邻接状态：邻居间的链路状态数据库同步完成，至此网络中所有路由器都有了相同的链路状态数据库，已掌握全网拓扑。

（3）计算最短路径生成路由表。

每台路由器基于链路状态数据库，使用最短路径优先（Short Path First，SPF）算法计算出一棵以自己为根的、无环的、拥有最短路径的“树”，产生到达目标网络的路由条目。

6.2.5　OSPF报文类型

OSPF共有5种报文类型，图6-6标出了OSPF运行各个阶段用到的报文类型。

类型1：问候（Hello）数据包，用于发现与维持邻居。

类型2：数据库描述（Database Description，DD）数据包，向邻居给出自己的链路状态数据库中所有链路状态项目的摘要信息，摘要信息是链路状态表中的所有路由器（Router-ID）。

类型3：链路状态请求（Link State Request，LSR）数据包，向对方请求缺少的某个路由器相关的链路状态的详细信息。

类型4：链路状态更新（Link State Update，LSU）数据包，发送详细的链路状态信息。路由器使用这种数据包将其链路状态通知给相邻路由器。在OSPF中，只有LSU需要显示确认。

类型5：链路状态确认（Link State Acknowledgement，LSAck）数据包，对LSU做确认。

6.2.6 OSPF三张表

OSPF有三张重要的表：OSPF邻居表、LSDB表和OSPF路由表。

OSPF在传递链路状态信息之前，需要建立邻居关系。邻居关系通过交互Hello报文建立。OSPF邻居表显示了OSPF路由器之间的邻居状态，使用display ospf peer可查看邻居表。

运行链路状态路由协议的路由器在网络中泛洪链路状态信息。在OSPF中，这些信息被称为LSA，LSDB会保存自己产生的以及从邻居收到的LSA信息，因此LSDB可以当作路由器对网络的完整认知。在华为设备上查看设备的LSDB的命令是display ospf lsdb。

OSPF根据LSDB中的数据，运行SPF算法并且得到一棵以自己为根的、无环的最短路径树。基于这棵树，OSPF能够发现到达网络中各个网段的最佳路径，从而得到路由信息并将其加载到OSPF路由表中。当然，这些OSPF路由表中的路由最终是否会被加载到全局路由表，还要经过进一步比较路由优先级等过程。在华为设备上查看设备的OSPF路由表的命令是display ospf routing。

6.2.7 OSPF区域

为了使OSPF能够用于规模很大的网络，OSPF将一个自治系统再划分为若干更小的范围，该范围叫作区域（area）。划分区域的好处，就是可以把洪泛法交换链路状态信息的范围控制在一个区域而不是整个自治系统，这就减少了整个网络上的通信量，从而减小链路状态数据库LSDB大小、提高网络的可扩展性以达到快速收敛。一个区域内部的路由器只需要知道本区域的完整网络拓扑，

而不需要知道其他区域的网络拓扑情况。为了使一个区域能够和本区域以外的区域进行通信，OSPF使用层次结构的区域划分。

当网络中包含多个区域时，OSPF协议有一个特殊的规定，即其中必须有一个Area 0，通常也叫作骨干区域（Backbone Area）。当设计OSPF网络时，一个很好的方法就是从骨干区域开始，然后再扩展到其他区域。骨干区域在所有其他区域的中心，即所有区域都必须与骨干区域物理或逻辑上相连。这种设计思想产生的原因是，OSPF协议要把所有区域的路由信息引入骨干区域，然后再将路由信息从骨干区域分发到非骨干区域中。

图6-7展示了一个有3个区域的自治系统（Autonomous System，AS）。每一个区域都有一个32位的区域标识符（用点分十进制表示）。一个区域的规模不能太大，区域内的路由器最好不超过200个。

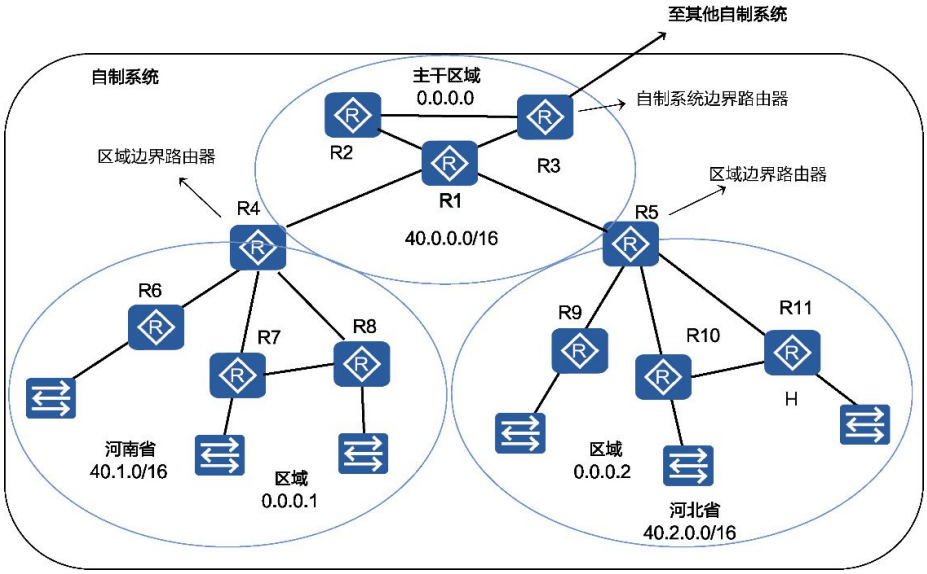


图6-7　自治系统和OSPF区域

如图6-7所示，使用多区域划分要和IP地址规划相结合，以确保一个区域的地址空间连续，这样才能在区域边界路由器上将一个区域的网络汇总成一条路由并通告给其他区域。

上层的区域叫作骨干区域，骨干区域的标识符规定为0.0.0.0。骨干区域的作用是连通其他下层的区域。从其他区域发来的信息都由区域边界路由器（Area Border Router，ABR）进行路由汇总。如图6-7所示，路由器R4和R5都是区域边界路由器。显然，每一个区域至少应当有一个区域边界路由器。骨干区域内的路由器叫作骨干路由器（Backbone Router），如R1、R2、R3、R4和R5。骨干路由器可以同时是区域边界路由器，如R4和R5。骨干区域内还要有一个路由器（图6-7中的R3）专门和本自治系统外的其他自治系统交换路由信息，这样的路由器叫作自治系统边界路由器（Autonomous System Boundary Router，ASBR）。

需要说明的是，ABR连接骨干区域和非骨干区域，ASBR连接其他AS。

6.3　配置OSPF协议

前面讲解了OSPF协议的特点和工作过程，本节来学习配置网络中的路由使用OSPF协议来构建路由表。

6.3.1　OSPF多区域配置

参照图6-8搭建网络环境，网络中的路由器按照图6-8中的拓扑连接，按照规划的网段来配置接口IP地址。一定要确保直连的路由器能够相互ping通。以下操作用于配置这些路由器使用OSPF协议来构造路由表。将这些路由器配置在一个区域中，如果只有一个区域，那么该区域只能是主干区域，区域编号是0.0.0.0，也可以写成0。

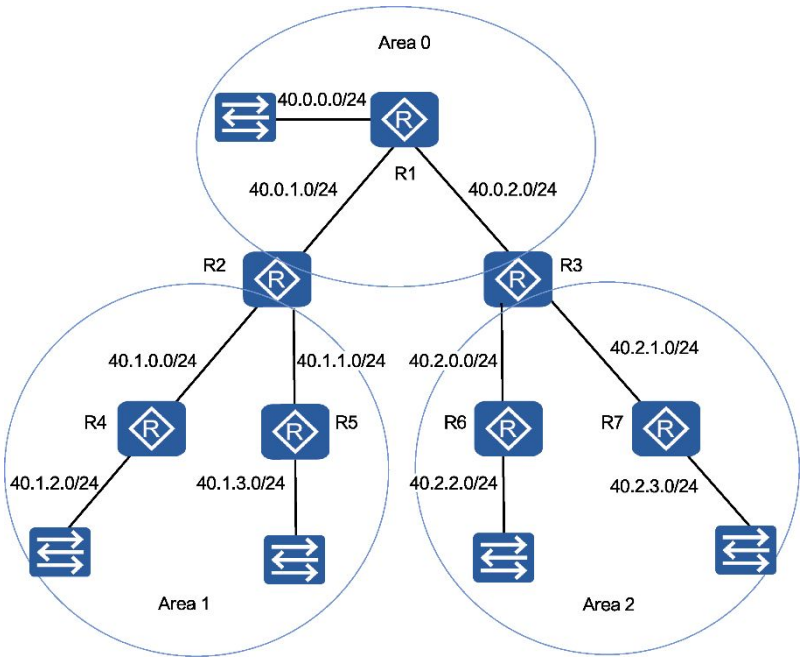


图6-8　多区域OSPF网络拓扑

路由器R1的配置如下，R1是骨干区域路由器。

```
<R1>display  router  id
RouterID:40.0.0.1                                                    --查看
路由器的当前ID
<R1>system
[R1]ospf  1  router-id  1.1.1.1                                  --启用OSPF  1进
程并指明使用的Router-ID
[R1-ospf-1]area  0.0.0.0                                                --创建区
域并进入区域  0.0.0.0
[R1-ospf-1-area-0.0.0.0]network  40.0.0.0  0.0.255.255  --指定工作在Area  0的
地址接口
[R1-ospf-1-area-0.0.0.0]quit
```

路由器R2的配置如下，R2是区域边界路由器，要指定工作在Area 0的接口和工作在Area 1的接口。

```
[R2]ospf  1  router-id  2.2.2.2
[R2-ospf-1]area  0
[R2-ospf-1-area-0.0.0.0]network  40.0.0.0  0.0.255.255    --指定工作在Area  0
的接口
[R2-ospf-1-area-0.0.0.0]quit

[R2-ospf-1]area  0.0.0.1
[R2-ospf-1-area-0.0.0.1]network  40.1.0.0  0.0.255.255    --指定工作在Area  1
的接口
[R2-ospf-1-area-0.0.0.1]quit
[R2-ospf-1]display  this
--显示OSPF  1的配置
[V200R003C00]
#
ospf  1  router-id  2.2.2.2
  area  0.0.0.0
    network  40.0.0.0  0.0.255.255
  area  0.0.0.1
    network  40.1.0.0  0.0.255.255
#
return
```

路由器R3的配置如下。

```
 [R3]ospf  1  router-id  3.3.3.3
[R3-ospf-1]area  0.0.0.0
[R3-ospf-1-area-0.0.0.0]network  40.0.0.0  0.0.255.255
[R3-ospf-1-area-0.0.0.0]quit
[R3-ospf-1]area  0.0.0.2
[R3-ospf-1-area-0.0.0.2]network  40.2.0.1  0.0.0.0    --写接口地址，wildcard-
mask为0.0.0.0
[R3-ospf-1-area-0.0.0.2]network  40.2.1.1  0.0.0.0    --写接口地址，wildcard-
mask为0.0.0.0
[R3-ospf-1-area-0.0.0.2]quit
```

路由器R4的配置如下。

```
[R4]ospf  1  router-id  4.4.4.4
[R4-ospf-1]area  1
[R4-ospf-1-area-0.0.0.1]net
[R4-ospf-1-area-0.0.0.1]network  40.1.0.0  0.0.255.255
[R4-ospf-1-area-0.0.0.1]quit
```

路由器R5的配置如下。

```
[R5]ospf  1  router-id  5.5.5.5
[R5-ospf-1]area  1
[R5-ospf-1-area-0.0.0.1]network  40.1.0.0  0.0.255.255
[R5-ospf-1-area-0.0.0.1]quit
```

路由器R6的配置如下。

```
[R6]ospf  1  router-id  6.6.6.6
[R6-ospf-1]area  2
[R6-ospf-1-area-0.0.0.2]network  40.2.0.0  0.0.255.255
[R6-ospf-1-area-0.0.0.2]quit
```

路由器R7的配置如下。

```
[R7]ospf  1  router-id  7.7.7.7
[R7-ospf-1]area  2
[R7-ospf-1-area-0.0.0.2]network  40.2.0.0  0.0.255.255
[R7-ospf-1-area-0.0.0.2]quit
```

6.3.2　查看OSPF协议的3张表

运行OSPF协议的路由器有3张表，分别是邻居表、链路状态表和OSPF路由表，下面就介绍这3张表。

先来查看R1路由器的邻居表。在系统视图下输入display ospf peer，可以显示邻居路由器信息，输入display ospf peer brief可以显示邻居路由器摘要信息。

```
<R1>display  ospf  peer  brief                    --显示邻居路由器摘要信息
             OSPF  Process  1  with  Router  ID  1.1.1.1
```

```
                              Peer  Statistic  Information
  ------------------------------------------------------------------------------
---
  Area  Id                      Interface
Neighbor  id            State
  0.0.0.0                    Serial2/0/0
2.2.2.2                    Full
  0.0.0.0                    Serial2/0/1
3.3.3.3                    Full
  ------------------------------------------------------------------------------
---
<R1>display  ospf  peer                                        --显示邻居详细信息
```

在Full状态下，路由器及其邻居会达到完全邻接状态。所有路由器和网络LSA都会交换，并且路由器链路状态表会达到同步状态。

显示链路状态表。以下命令显示链路状态表中有几个路由器通告了链路状态。通告链路状态的路由器就是AdvRouter。

```
<R1>display  ospf  lsdb

               OSPF  Process  1  with  Router  ID  1.1.1.1
                         Link  State  Database

                                            Area:  0.0.0.0
  Type            LinkState  ID        AdvRouter                    Age
Len      Sequence      Metric
  Router          2.2.2.2                 2.2.2.2
1260    48        80000011            48
  Router          1.1.1.1                 1.1.1.1
1218    84        80000013              1
  Router          3.3.3.3                 3.3.3.3
1253    48        80000010            48
  Sum-Net      40.1.3.0                 2.2.2.2                       301
28        80000001            49
  Sum-Net      40.1.2.0                 2.2.2.2                       221
28        80000001            49
  Sum-Net      40.1.1.0                 2.2.2.2                       932
28        80000001            48
  Sum-Net      40.1.0.255             2.2.2.2                        932
28        80000001            48
  Sum-Net      40.2.3.0                 3.3.3.3                       856
28        80000001            49
  Sum-Net      40.2.2.0                 3.3.3.3                       856
28        80000001            49
  Sum-Net      40.2.1.0                 3.3.3.3                       856
28        80000001            48
```

```
  Sum-Net      40.2.0.255             3.3.3.3                        856
28        80000001            48
```

从以上输出可以看到骨干区域路由器R1的链路状态表出现了Area 1和Area 2的子网信息。这些子网信息是由区域边界路由器通告到骨干区域的。在区域边界路由器上配置了路由汇总，这样Area 1、Area 2就被汇总成一条链路状态。

前面给大家讲了OSPF是怎样根据链路状态表计算最短路径的。链路状态表记录了运行OSPF的路由器有哪些，每个路由器连接几个网段（subnet），每个路由器有哪些邻居，通过什么链路连接（点到点还是以太网链路）。如果想查看完整的链路状态表，需要输入display ospf lsdb router命令，可以看到每个路由器的相关链路状态。

输入display ip routing-table可以查看路由表。Proto是通过OSPF协议学到的路由，OSPF协议的优先级（也就是pre）是10，Cost是通过带宽计算的到达目标网段的累计开销。

```
<R1>display  ip  routing-table  protocol  ospf
--查看OSPF路由
Route  Flags:  R  -  relay,  D  -  download  to  fib
------------------------------------------------------------------------------
---
Public  routing  table  :  OSPF
                      Destinations  :  8                Routes  :  8

OSPF  routing  table  status  :  <Active>
                     Destinations  :  8                Routes  :  8

Destination/Mask       Proto      Pre    Cost          Flags   NextHop
Interface

              40.1.0.0/24    OSPF        10      96                  D
40.0.1.2                Serial2/0/0
              40.1.1.0/24    OSPF        10      96                  D
40.0.1.2                Serial2/0/0
              40.1.2.0/24    OSPF        10      97                  D
40.0.1.2                Serial2/0/0
              40.1.3.0/24    OSPF        10      97                  D
40.0.1.2                Serial2/0/0
              40.2.0.0/24    OSPF        10      96                    D
40.0.2.2                Serial2/0/1
              40.2.1.0/24    OSPF        10      96                    D
40.0.2.2                Serial2/0/1
```

```
              40.2.2.0/24    OSPF        10      97                    D
40.0.2.2                Serial2/0/1
              40.2.3.0/24    OSPF        10      97                    D
40.0.2.2                Serial2/0/1

OSPF  routing  table  status  :  <Inactive>
                     Destinations  :  0                          Routes  :
0
```

输入以下命令，只显示OSPF协议生成的路由，能够看到通告者的ID——AdvRouter。可以看到直连的以太网开销默认为1，串口的默认开销为48。

```
  <R1>display  ospf  routing

               OSPF  Process  1  with  Router  ID  1.1.1.1
                          Routing  Tables

  Routing  for  Network
  Destination               Cost     Type                    NextHop
AdvRouter              Area
  40.0.0.0/24                1           Stub                   40.0.0.1
1.1.1.1                  0.0.0.0
  40.0.1.0/24               48          Stub                   40.0.1.1
1.1.1.1                  0.0.0.0
  40.0.2.0/24               48          Stub                   40.0.2.1
1.1.1.1                  0.0.0.0
  40.1.0.0/24               96          Inter-area     40.0.1.2
2.2.2.2                  0.0.0.0
  40.1.1.0/24               96          Inter-area     40.0.1.2
2.2.2.2                  0.0.0.0
  40.1.2.0/24               97          Inter-area     40.0.1.2
2.2.2.2                  0.0.0.0
  40.1.3.0/24               97          Inter-area     40.0.1.2
2.2.2.2                  0.0.0.0
  40.2.0.0/24               96          Inter-area     40.0.2.2
3.3.3.3                  0.0.0.0
  40.2.1.0/24               96          Inter-area     40.0.2.2
3.3.3.3                  0.0.0.0
  40.2.2.0/24               97          Inter-area     40.0.2.2
3.3.3.3                  0.0.0.0
  40.2.3.0/24               97          Inter-area     40.0.2.2
3.3.3.3                  0.0.0.0

  Total  Nets:  11
  Intra  Area:  3    Inter  Area:  8    ASE:  0    NSSA:  0
```

6.3.3 在区域边界路由器上进行路由汇总

在区域边界路由器R2上进行路由汇总。将Area 1汇总成40.1.0.0 255.255.0.0，开销指定为10，将Area 0汇总成40.0.0.0 255.255.0.0，指定开销为10。

```
 [R2]ospf  1
[R2-ospf-1]area  1
[R2-ospf-1-area-0.0.0.1]abr-summary  40.1.0.0  255.255.0.0  cost  10
[R2-ospf-1-area-0.0.0.1]quit

[R2-ospf-1]area  0
[R2-ospf-1-area-0.0.0.0]abr-summary  40.0.0.0  255.255.0.0  cost  10
[R2-ospf-1-area-0.0.0.0]quit
```

在区域边界路由器R3上进行路由汇总。将Area 2汇总成40.2.0.0 255.255.0.0，开销指定为20，将Area 0汇总成40.0.0.0 255.255.0.0，指定开销为10。

```
[R3]ospf  1
[R3-ospf-1]area  0
[R3-ospf-1-area-0.0.0.0]abr-summary  40.0.0.0  255.255.0.0  cost  10
[R3-ospf-1-area-0.0.0.0]quit
[R3-ospf-1]area  2
[R3-ospf-1-area-0.0.0.2]abr-summary  40.2.0.0  255.255.0.0  cost  20
[R3-ospf-1-area-0.0.0.2]quit
[R3-ospf-1]quit
```

在区域边界路由器上汇总后，在R1上查看OSPF链路状态，可以看到Area 1和Area 2在R1的链路状态表中只显示一条记录。

```
<R1>display  ospf  lsdb

             OSPF  Process  1  with  Router  ID  1.1.1.1
                         Link  State  Database

                                              Area:  0.0.0.0
  Type            LinkState  ID        AdvRouter                    Age
Len      Sequence      Metric
  Router          2.2.2.2                 2.2.2.2
1732    48        80000011            48
  Router          1.1.1.1                 1.1.1.1
1690    84        80000013              1
  Router          3.3.3.3                 3.3.3.3
1725    48        80000010            48
  Sum-Net      40.1.0.0                 2.2.2.2                      99
28          80000001           10
```

```
  Sum-Net       40.2.0.0                3.3.3.3                         26
28          80000001          20
```

在R1上显示OSPF协议生成的路由。可以看到Area 0和Area 1汇总成一条路由，开销分别是58和68，这和汇总时指定的开销有关。

```
<R1>display  ospf  routing

             OSPF  Process  1  with  Router  ID  1.1.1.1
                        Routing  Tables

  Routing  for  Network
  Destination               Cost    Type                  NextHop
AdvRouter              Area
  40.0.0.0/24                1          Stub                   40.0.0.1
1.1.1.1                  0.0.0.0
  40.0.1.0/24                48        Stub                  40.0.1.1
1.1.1.1                  0.0.0.0
  40.0.2.0/24                48        Stub                  40.0.2.1
1.1.1.1                  0.0.0.0
  40.1.0.0/16                58        Inter-area     40.0.1.2
2.2.2.2                  0.0.0.0
  40.2.0.0/16                68        Inter-area     40.0.2.2
3.3.3.3                  0.0.0.0

  Total  Nets:  5
  Intra  Area:  3    Inter  Area:  2    ASE:  0    NSSA:  0
```

6.3.4 OSPF协议配置排错

如果为网络中的路由器配置了OSPF协议，但在查看路由表后发现有些网段没有通过OSPF学到，那么需要检查路由器接口是否配置了正确的IP地址和子网掩码。除了进行这些常规检查，还要检查OSPF协议的配置。

要查看OSPF协议的配置，可以输入display current-configuration。

```
[R1]display  current-configuration
……
ospf  1  router-id  1.1.1.1
  area  0.0.0.0
    network  172.16.0.0  0.0.255.255
……
```

也可以进入ospf 1视图，输入display this，显示OSPF协议的配置。

```
[R1]ospf  1
  [R1-ospf-1]display  this
[V200R003C00]
#
ospf  1  router-id  1.1.1.1
  area  0.0.0.0
    network  172.16.0.0  0.0.255.255
#
return
```

输入display ospf interface可以查看运行OSPF协议的接口。如果发现缺少路由器的某个接口，那么需要使用network添加该接口。

```
<R1>display  ospf  interface

        OSPF  Process  1  with  Router  ID  1.1.1.1
              Interfaces

  Area:  0.0.0.0                (MPLS  TE  not  enabled)
  IP  Address            Type                  State        Cost         Pri
DR                          BDR
  172.16.1.1            Broadcast              DR             1
1          172.16.1.1           0.0.0.0
  172.16.0.1            P2P                    P-2-P          48
1          0.0.0.0                0.0.0.0
  172.16.0.17          P2P                    P-2-P          48           1
0.0.0.0                0.0.0.0
```

可以看到，配置OSPF协议时用network添加的3个网段和所属的区域。如果network后面的3个网段和路由器的接口所在的网段不一致，则该接口就不能发送和接收OSPF协议相关数据包，该网段也不会包含在链路状态中。或者，如果network后面的区域编号和相邻路由器配置的区域编号不一致，那也不能交换链路状态信息，也可能导致错误。

如果配置OSPF时network写错网段，可以使用undo network命令删除该网段，然后用network添加正确的网段。

可以在路由器上使用以下命令取消192.168.0.0/24网段参与OSPF协议。

```
[R3]ospf  1
[R3-ospf-1]display  this
[V200R003C00]
#
```

```
ospf  1  router-id  3.3.3.3
  area  0.0.0.0
    network  172.16.0.6  0.0.0.0
    network  172.16.0.9  0.0.0.0
    network  172.16.2.1  0.0.0.0
#
return
[R3-ospf-1]area  0
[R3-ospf-1-area-0.0.0.0]undo  network  172.16.2.1  0.0.0.0
```

6.4　虚拟路由冗余协议（VRRP）

虚拟路由冗余协议（Virtual Router Redundancy Protocol，VRRP）是由IETF提出的解决局域网中配置静态网关出现单点失效现象的路由协议，1998年已推出正式的RFC2338协议标准。

VRRP广泛应用在边缘网络中，VRRP的作用是充当网络中的一个默认网关，可以说计算机定义的网关不生效的话，则整个网络都用不了，只能访问同一个VLAN内的计算机。VRRP解决的问题就是，通过VRRP技术协商让连接网络的多个路由器的接口虚拟一个IP地址出来，充当该网络的网关。这样做的好处就是，网络中的计算机只需要指定路由器接口虚拟的那个IP地址作为网关即可，当主设备出现故障后，该虚拟IP地址会自动切换到备用设备上，对计算机来说是透明的。

如图6-9所示，企业内网为了确保Internet连接的可靠性，有两个路由器连接Internet。AR1作为连接Internet的主链路，AR3作为内网连接Internet的备用链路。当主链路断开时，内网计算机通过AR3走备用链路访问Internet。

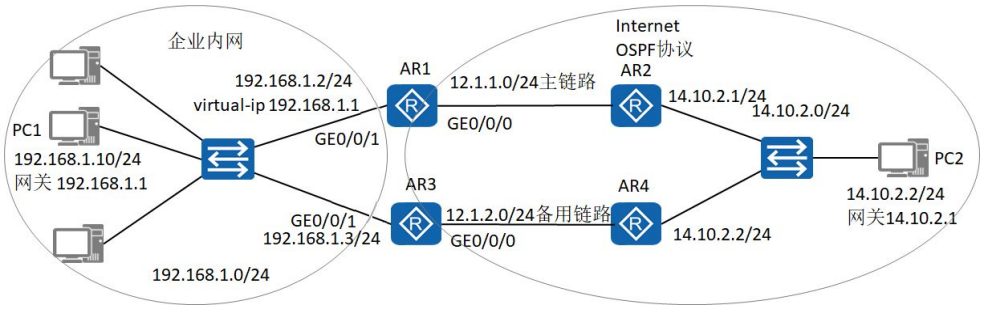


图6-9　VRRP实验环境

这就要求配置AR1的GE0/0/1接口和AR3的GE0/0/1接口使用VRRP配置一个虚拟IP作为内网的网关，本例中虚拟IP为192.168.1.1。AR1、AR2、AR3和AR4均运行OSPF动态路由协议。

在AR1上的配置如下。

```
<Huawei>sys
[Huawei]sysname  AR1
[AR1]interface  GigabitEthernet  0/0/1
[AR1-GigabitEthernet0/0/1]ip  add
[AR1-GigabitEthernet0/0/1]ip  address  192.168.1.2  24
[AR1-GigabitEthernet0/0/1]quit
[AR1]interface  GigabitEthernet  0/0/0
[AR1-GigabitEthernet0/0/0]ip  address  12.1.1.1  24
[AR1-GigabitEthernet0/0/0]quit
[AR1]ospf  router-id  1.1.1.1
[AR1-ospf-1-area-0.0.0.0]network  192.168.1.0  0.0.0.255
[AR1-ospf-1-area-0.0.0.0]network  12.1.1.0  0.0.0.255
[AR1-ospf-1-area-0.0.0.0]quit
[AR1-ospf-1]quit
```

在AR2上的配置如下。

```
<Huawei>sys
[Huawei]sysname  AR2
[AR2]interface  GigabitEthernet  0/0/0
[AR2-GigabitEthernet0/0/0]ip  address  12.1.1.2  24
[AR2-GigabitEthernet0/0/0]interface  GigabitEthernet  0/0/1
[AR2-GigabitEthernet0/0/1]ip  address  14.10.2.1  24
[AR2-GigabitEthernet0/0/1]quit
[AR2]ospf  router-id  2.2.2.2
[AR2-ospf-1-area-0.0.0.0]network  12.1.1.0  0.0.0.255
[AR2-ospf-1-area-0.0.0.0]network  14.10.2.0  0.0.0.255
[AR2-ospf-1-area-0.0.0.0]quit
```

在AR3上的配置如下。

```
[Huawei]sys
[Huawei]sysname  AR3
[AAR3]interface  GigabitEthernet  0/0/1
[AAR3-GigabitEthernet0/0/1]ip  address  192.168.1.3  24
[AR3-GigabitEthernet0/0/1]interface  GigabitEthernet  0/0/0
[AR3-GigabitEthernet0/0/0]ip  address  12.1.2.1  24.
[AR3-GigabitEthernet0/0/0]quit
[AR3]ospf  router-id  3.3.3.3
[AR3-ospf-1]area  0
[AR3-ospf-1-area-0.0.0.0]network  192.168.1.0  0.0.0.255
[AR3-ospf-1-area-0.0.0.0]network  12.1.2.0  0.0.0.255
```

在AR4上的配置如下。

```
[Huawei]sysname  AR4
[AR4]interface  GigabitEthernet  0/0/0
```

```
[AR4-GigabitEthernet0/0/0]ip address 12.1.2.2 24
[AR4-GigabitEthernet0/0/0]interface GigabitEthernet 0/0/1
[AR4-GigabitEthernet0/0/1]ip address 14.10.2.254 24
[AR4-GigabitEthernet0/0/1]quit
[AR4]ospf router-id 4.4.4.4
[AR4-ospf-1]area 0
[AR4-ospf-1-area-0.0.0.0]network 14.10.2.0 0.0.0.255
[AR4-ospf-1-area-0.0.0.0]network 12.1.2.0 0.0.0.255
```

在AR1上配置VRRP。配置AR1在接口GE 0/0/1配置虚拟IP地址，一个虚拟地址就相当于一个虚拟路由器，一个路由器可以创建多个虚拟路由器，用vrid标识，即Virtual Router ID。使用priority指定优先级，AR1为连接Internet的主链路，优先级设置为120，默认优先级为100，如果连接Internet的接口GE0/0/0接口断开或down掉，将优先级减少40。Preempt-mode参数用来设置当主链路恢复后延迟多少秒恢复到主链路。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip 192.168.1.1
[AR1-GigabitEthernet0/0/1]vrrp vrid 1 priority ?
    INTEGER<1-254>    The level of priority(default is 100)
[AR1-GigabitEthernet0/0/1]vrrp vrid 1 priority 120
[AR1-GigabitEthernet0/0/1]vrrp vrid 1 track interface GigabitEthernet
0/0/0 reduced 40
[AR1-GigabitEthernet0/0/1]vrrp vrid 1 preempt-mode ?
    disable    Cancel current configuration
    timer        Specify timer
[AR1-GigabitEthernet0/0/1]vrrp vrid 1 preempt-mode timer delay 30
[AR1-GigabitEthernet0/0/1]
```

在AR3上配置VRRP。AR3接口GE0/0/1的VRRP优先级使用默认值100。这样当主链路不可用后，AR1的GE0/0/1接口的VRRP优先级就降为80，虚拟IP地址就绑定到AR3的GE0/0/1接口，AR3就成为连接Internet的主链路。不设置优先级，就使用默认优先级，在备用链路的路由器上不用设置跟踪接口，也不用使用Preempt-mode参数设置恢复时间。

```
[RA3]interface GigabitEthernet 0/0/1
[RA3-GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip 192.168.1.1
```

在AR1上查看VRRP 1的状态。

```
<R1>display vrrp 1
    GigabitEthernet0/0/1 | Virtual Router 1
        State : Master
        Virtual IP : 192.168.1.1
        Master IP : 192.168.1.2
        PriorityRun : 120
        PriorityConfig : 120
        MasterPriority : 120
        Preempt : YES      Delay Time : 30 s
        TimerRun : 1 s
        TimerConfig : 1 s
        Auth type : NONE
        Virtual MAC : 0000-5e00-0101
        Check TTL : YES
        Config type : normal-vrrp
        Backup-forward : disabled
        Track IF : GigabitEthernet0/0/0      Priority reduced : 40
        IF state : UP
        Create time : 2020-04-11 16:54:08 UTC-08:00
        Last change time : 2020-04-11 17:17:30 UTC-08:00
```

6.5　习题

1．以下关于OSPF协议的描述中，最准确的是（　　）。

A．OSPF协议根据链路状态法计算最佳路由

B．OSPF协议是用于自治系统之间的外部网关协议

C．OSPF协议不能根据网络通信情况动态地改变路由

D．OSPF协议只能适用于小型网络

2．关于OSPF协议，下面的描述中不正确的是（　　）。

A．OSPF是一种链路状态协议

B．OSPF使用链路状态公告（LSA）扩散路由信息

C．OSPF网络中用区域1表示主干网段

D．OSPF路由器中可以配置多个路由进程

3．OSPF支持多进程，如果不指定进程号，则默认使用的进程号是（　　）。

A．0

B．1

C．10

D．100

4．如图6-10所示，为网络中的路由器配置了OSPF协议，在路由器A和B上进行以下配置。

```
[A]ospf  1  router-id  1.1.1.1
[A-ospf-1]area  0.0.0.0
[A-ospf-1-area-0.0.0.0]network  172.16.0.0  0.0.255.255
[A-ospf-1-area-0.0.0.0]network  192.168.0.0  0.0.0.255
[B]ospf  1  router-id  1.1.1.2
[B-ospf-1]area  0.0.0.0
[B-ospf-1-area-0.0.0.0]network  192.168.0.0  0.0.255.255
```

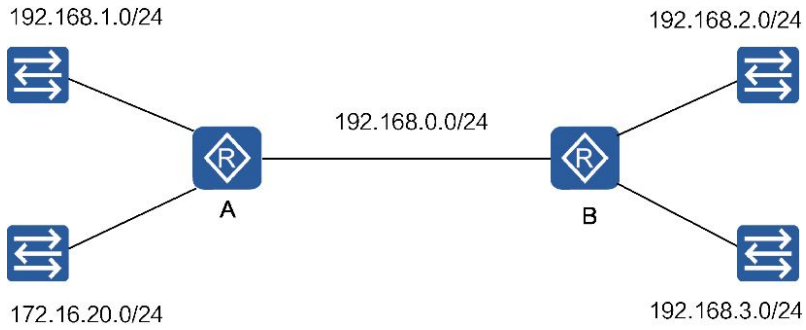


图6-10　网络拓扑

以下哪些说法不正确？（　　）

A．在路由器B上能够通过OSPF协议学到到172.16.0.0/24网段的路由

B．在路由器B上能够通过OSPF协议学到到192.168.1.0/24网段的路由

C．在路由器A上能够通过OSPF协议学到到192.168.2.0/24网段的路由

D．在路由器A上能够通过OSPF协议学到到192.168.3.0/24网段的路由

5．在一台路由器上配置OSPF，必须手动进行的配置有（　　）。（选择3个答案）

A．配置Router-ID

B．开启OSPF进程

C．创建OSPF区域

D．指定每个区域中包含的网段

6．在VRP平台上，直连路由、静态路由、RIP、OSPF的默认协议优先级从高到低依次是（　　）。

A．直连路由、静态路由、RIP、OSPF

B．直连路由、OSPF、静态路由、RIP

C．直连路由、OSPF、RIP、静态路由

D．直连路由、RIP、静态路由、OSPF

7．管理员在某台路由器上配置OSPF，但该路由器上未配置back接口，则以下关于Router-ID的描述中正确的（　　）。

A．该路由器物理接口的最小IP地址将会成为Router-ID

B．该路由器物理接口的最大IP地址将会成为Router-ID

C．该路由器管理接口的IP地址将会成为Router-ID

D．该路由器的优先级将会成为Router-ID

8．以下关于OSPF中Router-ID的描述中正确的是（　　）。

A．同一区域内Router-ID必须相同，不同区域内的Router-ID可以不同

B．Router-ID必须是路由器某接口的IP地址

C．必须通过手动配置的方式来指定Router-ID

D．OSPF协议正常运行的前提条件是路由器有Router-ID

9．一台路由器通过RIP、OSPF和静态路由学习到了到达同一目标地址的路由。默认情况下，VRP将最终选择通过哪种协议学习到的路由？（　　）

A．RIP

B．OSPF

C．RIP

D．静态路由

10．假定配置如下所示：

```
[R1]ospf
[R1-ospf-1]area  1
[R1-ospf-1-area-0.0.0.1]network  10.0.12.0  0.0.0.255
```

管理员在路由器R1上配置了OSPF，但路由器R1学习不到其他路由器的路由，那么可能的原因是（　　）。（选择3个答案）

A．此路由器配置的区域ID和它的邻居路由器的区域ID不同

B．此路由器没有配置认证功能，但是邻居路由器配置了认证功能

C．此路由器有配置时没有配置OSPF进程号

D．此路由器在配置OSPF时没有宣告连接邻居的网络

11．OSPFv3使用哪个区域号标识骨干区域？（　　）

A．0

B．3

C. 1

D. 2

第7章　交换机组网

本章内容

- 交换机常规配置
- 交换机端口安全
- 生成树协议
- 创建和管理VLAN
- 实现VLAN间路由
- 端口隔离技术
- 链路聚合

本章讲解交换机组网的相关技术，包括设置交换机管理地址和交换机登录密码，以及允许telnet配置交换机。

交换机基于MAC地址转发帧，可以设置交换机端口以启用安全功能，交换机端口可以限制连接的计算机数量并绑定MAC地址。可以设置交换机监控端口以监控网络中的流量。

在进行交换机组网时，为了避免单台设备的故障造成网络长时间中断，往往需要设计成有冗余的网络结构，比如双汇聚层网络，但这样会形成环路。为了避免广播帧在环路中无限转发，交换机使用生成树协议来阻断环路。本章讲解生成树协议的工作过程，并指定根网桥和备用根网桥。

交换机组网使网段划分变得非常灵活，可以根据部门而不是物理位置划分网段，一个部门的计算机使用一个网段，占用一个VLAN。本章先讲解使用一个交换机划分多个VLAN，再讲解跨交换机的VLAN、交换机的端口类型，使用三层交换实现VLAN间路由以及使用单臂路由器实现VLAN间路由。

端口隔离技术可以使同一个VLAN内的计算机不能相互通信，只能访问Internet，这种技术在很多单位用得到。

交换机之间的多条物理链路可以使用Eth-Trunk技术捆绑在一起，形成一条逻辑链路，从而实现带宽加倍、流量负载均衡和链路容错。

7.1　交换机常规配置

在连接计算机时，交换机的端口不能设置IP地址，也不能充当计算机的网关。但是为了远程管理交换机，需要给交换机设置管理地址。该地址不充当计算机的网关，目的就是使用telnet远程管理交换机。

如图7-1所示，交换机LSW1和LSW2的管理地址分别是它们所在网段的一个地址，并且需要设置网关。

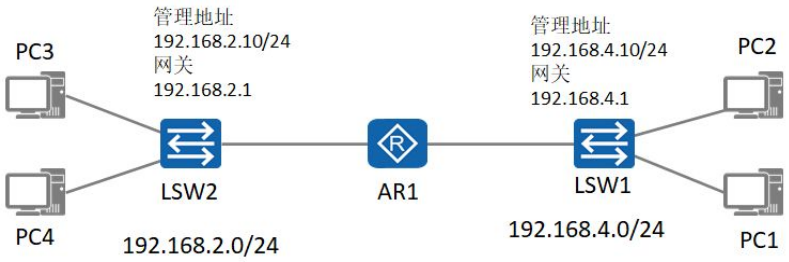


图7-1　交换机的管理地址

下面为LSW1配置管理地址。默认情况下交换机的所有接口都在VLAN 1，交换机的每个VLAN都有一个对应的虚拟接口（Vlanif），可以为虚拟接口设置IP地址以作为管理地址，关于VLAN的知识本章后面会讲到。

```
[LSW1]interface Vlanif 1                                --为VLanif 1接口设置管理地址
[LSW1-Vlanif1]ip address 192.168.4.10 24                --设置管理地址
[LSW1-Vlanif1]quit
[LSW1]ip route-static 0.0.0.0 0.0.0.0 192.168.4.1       --添加默认路由，也就是网关
```

设置Console口的身份验证模式和密码，和配置路由器的Console口的方法类似。

```
[LSW1]user-interface console 0
[LSW1-ui-console0]authentication-mode password
[LSW1-ui-console0]set authentication password cipher 91xueit
[LSW1-ui-console0]idle-timeout 5 30
```

设置VTY接口的身份验证模式和密码。

```
[LSW1]user-interface vty 0 4
[LSW1-ui-vty0-4]authentication-mode password
[LSW1-ui-vty0-4]set authentication password cipher 51cto
[LSW1-ui-vty0-4]idle-timeout 3 30
```

7.2　交换机端口安全

如果企业网络对安全要求比较高，那么通常会对接入网络的计算机进行控制。在交换机上启用端口安全，以对接入的计算机进行控制。

7.2.1　交换机端口安全详解

- 启用端口安全。

在交换机接口上激活Port-Security后，该接口就有了安全功能，例如能够限制接口的最大MAC地址数量，从而限制接入的主机数量；也可以将接口和MAC地址绑定，从而实现接入安全。

- 保护措施（protect-action）。

如果违反了端口的安全设置，比如一个端口的MAC地址数量超过设定数量，或这个端口绑定的MAC地址有变化，那么该端口将会启动保护措施。

保护措施有protect（丢弃违反安全设置的帧）、restrict（丢弃违反安全设置的帧并产生警报）、shutdown（关闭端口，需要人工启用端口才能恢复）3种，默认是restrict。

- Port-Security与Sticky MAC地址。

配置端口和进行MAC地址绑定的工作量很大。可以让交换机将动态学习到的MAC地址变成“粘滞状态”。可以简单理解为：先动态地学，学完之后再将MAC地址和端口粘起来（进行绑定），形成“静态”条目。

7.2.2　配置交换机端口安全

如图7-2所示，在LSW2交换机上设置端口安全，端口Ethernet 0/0/1只允许连接PC1，端口Ethernet 0/0/2只允许连接PC2，端口Ethernet 0/0/3只允许连接PC3，端口Ethernet 0/0/4最多只允许连接两台计算机且只能是PC4和PC5。若违反安全规则，端口关闭（shutdown）。

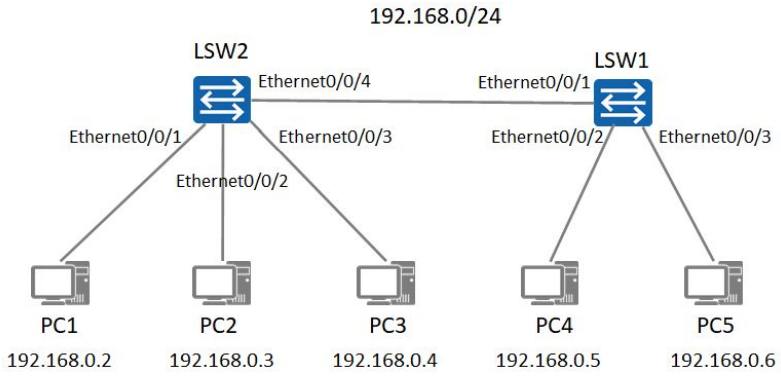


图7-2　配置交换机端口安全

以下操作将设置交换机LSW2，为Ethernet 0/0/1～Ethernet 0/0/3启用端口安全，每个端口只允许连接一个MAC地址（计算机），端口和MAC地址的绑定通过Sticky方式实现。为Ethernet 0/0/4启用端口安全，设置最多允许两个MAC地址，并且人工绑定PC4和PC5两个MAC地址。

LSW2上的配置如下。

```
[Huawei]sysname LSW2                    --改名为LSW2
```

在PC1上ping PC2、PC3、PC4、PC5，LSW2完成了MAC地址表的构建。

```
[LSW2]display mac-address               --显示MAC地址表
MAC address table of slot 0:
-------------------------------------------------------------------------------
-
MAC Address    VLAN/       PEVLAN CEVLAN Port           Type       LSP/LSR-ID
               VSI/SI                                               MAC-Tunnel
-------------------------------------------------------------------------------
-
5489-9854-3d93  1           -      -      Eth0/0/1      dynamic    0/-
5489-9813-531a  1           -      -      Eth0/0/2      dynamic    0/-
5489-9889-60df  1           -      -      Eth0/0/3      dynamic    0/-
5489-9809-119b  1           -      -      Eth0/0/4      dynamic    0/-
```

```
5489-98bd-0b2c  1           -       -       Eth0/0/4      dynamic    0/-
-------------------------------------------------------------------------------
-
Total matching items on slot 0 displayed = 5
```

可以看到MAC地址表列出了每个MAC地址所属的VLAN、对应的接口和类型。

设置Ethernet 0/0/1～Ethernet 0/0/3端口安全，将现有计算机的MAC地址和端口绑定。可以逐个端口进行设置，也可以定义一个端口组，添加端口成员，进行批量安全设置。

```
[LSW2]port-group 1to3                       --定义端口组1to3
[LSW2-port-group-1to3]group-member Ethernet 0/0/1 to Ethernet 0/0/3  --添加成
员
[LSW2-port-group-1to3]display this          --显示端口组设置
#
port-group 1to3
 group-member Ethernet 0/0/1
 group-member Ethernet 0/0/2
 group-member Ethernet 0/0/3
#
Return
```

对于以下操作，步骤不能少，且顺序不能颠倒。

```
[LSW2-port-group-1to3]port-security enable                  --启用端口安全
[LSW2-port-group-1to3]port-security protect-action shutdown --违反安全规定，关闭
端口
[LSW2-port-group-1to3]port-security mac-address sticky --将现有端口与对应的MAC地
址绑定
[LSW2-port-group-1to3]quit
```

交换机的MAC地址表中的条目有老化时间，默认为300秒。如果某条目没有被刷新，那么300秒后就会被从MAC地址表中清除。再次在PC1上ping PC2、PC3、PC4、PC5，交换机会自动重新构建MAC地址表。

查看MAC地址表，可以看到端口Ethernet 0/0/1～Ethernet 0/0/3的Type为sticky，端口Ethernet 0/0/4的Type依然是dynamic。

```
[LSW2]display mac-address vlan 1        --只显示VLAN 1的MAC地址表
MAC address table of slot 0:
-------------------------------------------------------------------------------
-
```

```
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type     LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
--------------------------------------------------------------------------------
-
5489-9854-3d93  1           -      -      Eth0/0/1        sticky    -
5489-9889-60df  1           -      -      Eth0/0/3        sticky    -
5489-9813-531a  1           -      -      Eth0/0/2        sticky    -
--------------------------------------------------------------------------------
-
Total matching items on slot 0 displayed = 3

MAC address table of slot 0:
--------------------------------------------------------------------------------
-
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type     LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
--------------------------------------------------------------------------------
-
5489-9809-119b 1           -      -      Eth0/0/4        dynamic   0/-
5489-98bd-0b2c 1           -      -      Eth0/0/4        dynamic   0/-
--------------------------------------------------------------------------------
-
Total matching items on slot 0 displayed = 2
```

设置交换机的Eth0/0/4端口安全：只允许连接两台计算机。

```
[LSW2]interface Ethernet 0/0/4                          --接入接口视图
[LSW2-Ethernet0/0/4]port-security enable
[LSW2-Ethernet0/0/4]port-security protect-action shutdown
[LSW2-Ethernet0/0/4]port-security max-mac-num 2         --设置最大数量
```

再次查看MAC地址表，可以看到端口Ethernet 0/0/4的Type为security，说明启用了端口安全。

```
[LSW2]display mac-address
MAC address table of slot 0:
--------------------------------------------------------------------------------
-
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type     LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
--------------------------------------------------------------------------------
-
5489-9813-531a 1           -      -      Eth0/0/2        sticky    -
5489-9809-119b 1           -      -      Eth0/0/4        security  -
5489-98bd-0b2c 1           -      -      Eth0/0/4        security  -
5489-9889-60df 1           -      -      Eth0/0/3        sticky    -
5489-9854-3d93 1           -      -      Eth0/0/1        sticky    -
--------------------------------------------------------------------------------
-
Total matching items on slot 0 displayed = 5
```

上面的设置只是指定了Ethernet 0/0/4端口的MAC地址数量。如果进一步打算将Ethernet 0/ 0/4 端口和指定的两个MAC地址绑定，就需要在端口视图中启用sticky，并绑定MAC地址。

因为前面设置Ethernet 0/0/4端口对应的MAC地址的最大数量为2，所以这里可以设置两个MAC地址。默认只允许1个端口绑定1个MAC地址。

```
[LSW2]interface Ethernet 0/0/4                                          --接入接口视图
[LSW2-Ethernet0/0/4]port-security mac-address sticky                    --启用sticky
[LSW2-Ethernet0/0/4]port-security mac-address sticky 5489-9809-119b vlan 1 --绑定MAC地址
[LSW2-Ethernet0/0/4]port-security mac-address sticky 5489-98bd-0b2c vlan 1 --绑定MAC地址
```

以上操作设置了交换机端口安全。若违反安全规则，那么端口将处于关闭状态，需要运行undo shutdown启用端口。

运行以下命令，清除端口的全部配置。配置清除后，端口将处于关闭状态，需要执行undo shutdown重新启用端口。

```
[LSW2]clear configuration interface Ethernet 0/0/4
```

7.2.3 镜像端口监控网络流量

如图 7-3 所示，如果打算在PC4上安装抓包工具或流量监控软件来监控网络中的计算机上网流量，那么PC4只能捕获自己发送和接收的数据包，PC1、PC2、PC3的上网流量由交换机直接转发到路由器的GE0/0/0端口，PC4上的抓包工具或流量监控软件是没有办法捕获这些数据包的。

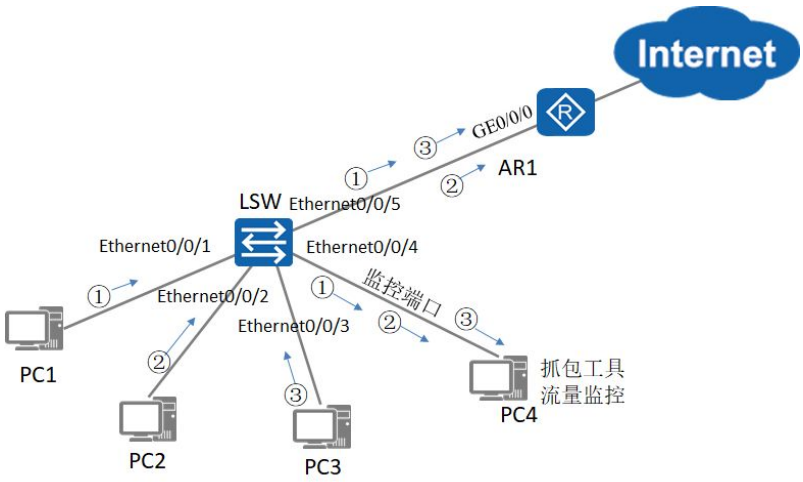


图7-3　镜像端口监控网络流量

为了让PC4上的抓包工具或流量监控软件能够捕获分析内网计算机访问Internet的流量，可以将交换机的Ethernet 0/0/4端口设置为监控端口，为Ethernet 0/0/5端口指定镜像端口（监控端口）。这样进出Ethernet 0/0/5端口的帧会同时转发给Ethernet 0/0/4端口。

由于在eNSP软件中模拟的交换机不支持镜像端口功能，因此我们使用AR1220路由器替代交换机来做镜像端口实验，如图7-4所示。

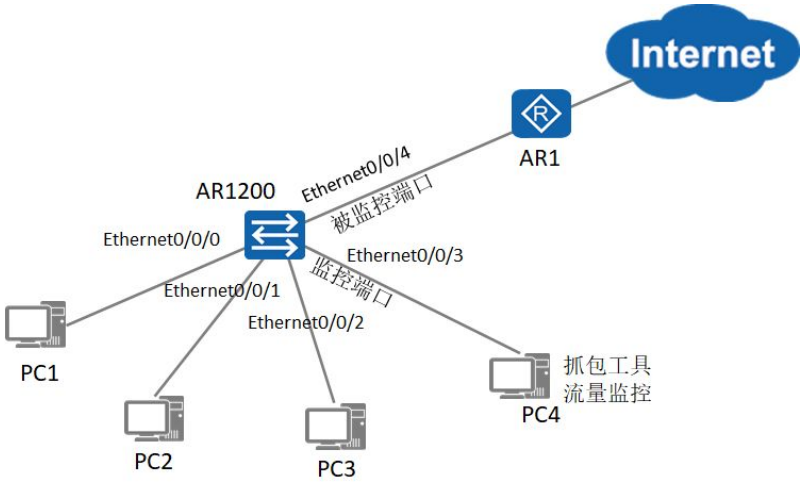


图7-4　通过AR1220路由器做镜像端口实验

```
[AR1200]observe-port interface Ethernet 0/0/3                          --指定监控端口
[AR1200]interface Ethernet 0/0/4
[AR1200-Ethernet0/0/4]mirror to observe-port ?
  both      Assign Mirror to both inbound and outbound of an interface --出入
端口的流量
  inbound   Assign Mirror to the inbound of an interface          --进端口的流量
  outbound  Assign Mirror to the outbound of an interface         --出端口的流量
[AR1200-Ethernet0/0/4]mirror to observe-port both --将出入端口的流量同时发送到监控
端口
```

验证镜像端口，捕获PC4 Ethernet 0/0/1端口的数据包，用PC1 ping网关192.168.0.1，可以看到捕获了PC1到网关的数据包。

注意：华为交换机只能设置一个observe-port监控端口。如果打算取消监控端口，需要先在被监视端口上取消镜像，然后再取消监控端口，配置命令如下。

```
[AR1200]interface Ethernet 0/0/4
[AR1200-Ethernet0/0/4]undo mirror both
[AR1200-Ethernet0/0/4]quit
[AR1200]undo observe-port
```

7.3　生成树协议

7.3.1　交换机组网环路问题

如图7-5所示，企业组建局域网，接入层交换机连接汇聚层交换机，如果汇聚层交换机出现故障，两台接入层交换机就不能相互访问，这就是单点故障。某些企业和单位不允许因设备故障造成网络长时间中断，为了避免汇聚层交换机单点故障，在组网时通常会部署两台汇聚层交换机。如图7-6所示，当汇聚层交换机1出现故障时，接入层的2台交换机可以通过汇聚层交换机2进行通信。

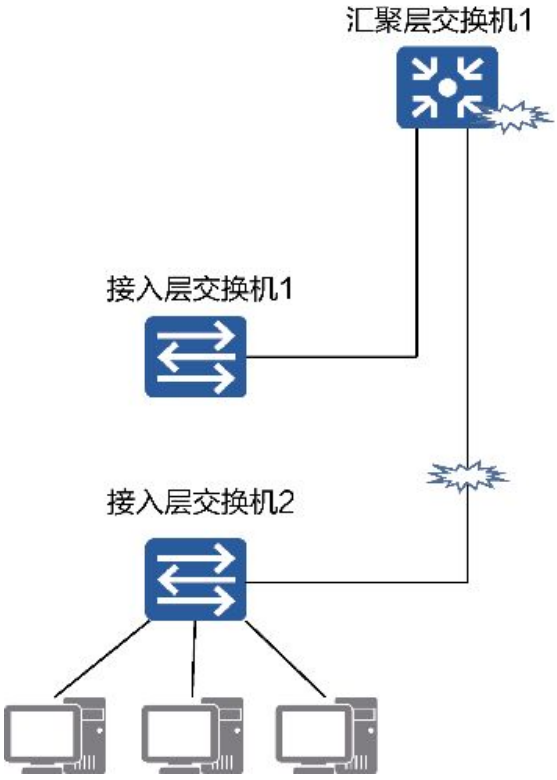


图7-5　单汇聚层组网

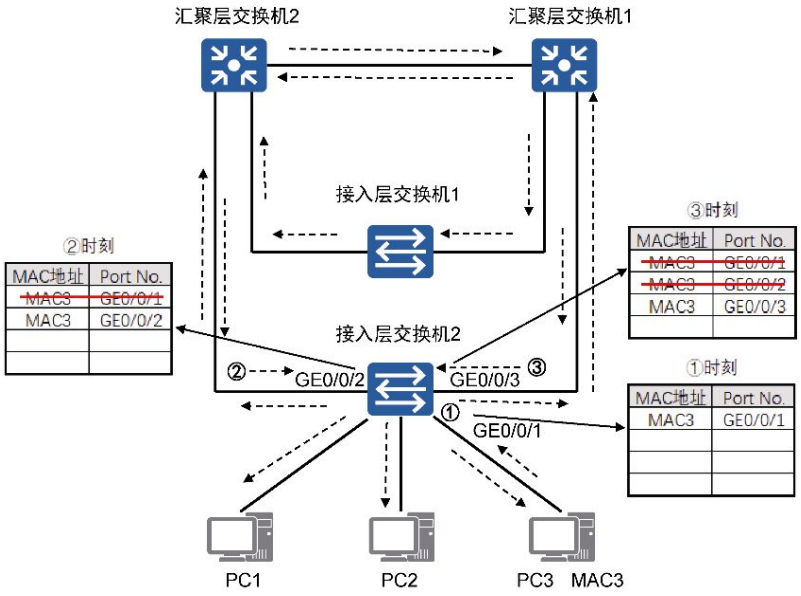


图7-6　双汇聚层组网

这样一来，交换机组建的网络则会形成环路。如图7-6所示，如果网络中计算机PC3发送广播帧，广播帧会在环路中一直转发，占用交换机的接口带宽，消耗交换机的资源，网络中的计算机会一直重复收到该帧，从而影响计算机接收正常通信的帧，这就是广播风暴。

交换机组建的网络如果有环路，还会出现交换机MAC地址表的快速翻摆。如图7-6所示，在①时刻接入层交换机2的GE0/0/1接口收到了PC3的广播帧，会在MAC地址表添加一条MAC3和GE0/0/1接口的映射。该广播帧会从接入层交换机2的GE0/0/3和GE0/0/2接口发送出去。在②时刻接入层交换机2的GE0/0/2从汇聚层交换机收到该广播帧，将MAC地址表中MAC3对应的端口修改为GE0/0/2。在③时刻接入层交换机2的GE0/0/3接口从汇聚层交换机1收到该广播帧，将MAC地址表中MAC3对应的端口更改为GE0/0/3。这样一来，接入层交换机2的MAC地址表中关于PC3的MAC地址的表项内容就会无休止地、快速地变来变去，这就是翻摆现象。接入层交换机1和汇聚层交换机1、2的MAC地址表也会出现完全一样的快速翻摆现象。MAC地址表的快速翻摆会大量消耗交换机的处理资源，甚至可能会导致交换机瘫痪。

这就要求交换机能够有效解决环路的问题。交换机使用生成树协议来阻断环路，大家都知道树型结构是没有环路的。

7.3.2 生成树协议概述

STP（Spanning Tree Protocol）是生成树协议的英文缩写，是在IEEE 802.1D中定议的数据链路层协议，可应用于计算机网络中树形拓扑结构的建立，主要作用是防止网桥网络中的冗余链路形成环路工作。生成树协议适用于所有厂商的网络设备，在配置和体现功能强度上有所差别，但是其原理和应用效果是一致的。

通过在交换机之间传递网桥协议数据单元（Bridge Protocol Data Unit，BPDU），并采用STA生成树算法选举根桥、根端口和指定端口的方式，可以将网络形成一个树形结构的网络，其中，根端口、指定端口都处于转发状态，其他端口处于禁用状态。如果网络拓扑发生改变，将重新计算生成树拓扑。生成树协议的存在，既解决了核心层网络需要冗余链路的网络健壮性要求，又解决了冗余链路形成的物理环路而导致的“广播风暴”问题。

生成树协议有3个版本，具体如下。

- CTP--Common Spanning Tree。

CST的协议号有802.1D，如果交换机运行在CST模式下，那么不管交换机中有多少个VLAN，所有的流量都会走相同的路径。

- RSTP--Rapid Spanning Tree Protocol。

RSTP称为快速生成树协议，协议号为802.1W。在运行CST时，接口的状态有Blocking、Listening、Disabled、Learning、Forwarding几种状态，其中Blocking、Listening、Disabled状态是不发送数据的。RSTP将这三种状态归为

一个状态，那就是Discarding状态，所以在RSTP中，接口的状态只有三种，分别是Discarding、Learning、Forwarding。

在CST模式中，如果根交换机失效了，那么需要等待50s才可以启用block端口；而RSTP只需要6s便可以发现根交换机失效。一旦发现根交换机失效，RSTP会立刻启用discarding端口。

- MSTP--Mutiple Spanning Tree Protocol。

RSTP和STP存在同一个缺陷，即局域网内所有的VLAN共享一棵生成树，链路被阻塞后将不承载任何流量，从而造成带宽浪费。多生成树协议（Multiple Spanning Tree Protocol，MSTP）是IEEE 802.1s中定义的一种新型生成树协议。MSTP中引入了“实例”（instance）和“域”（region）的概念。所谓“实例”，就是多个VLAN的一个集合，这种将多个VLAN捆绑到一个实例中的方法可以节省通信开销和资源占用率。MSTP中各个实例拓扑的计算是独立的，在这些实例上就可以实现负载均衡。使用的时候，可以把多个相同拓扑结构的VLAN映射到某个实例中，这些VLAN在端口上的转发状态将取决于对应实例在MSTP中的转发状态。

华为交换机生成树协议默认使用MSTP，本课程重点讲解STP，也就是CTP，在华为路由器上CTP就是STP。在描述STP协议之前，我们还需要了解几个基本术语：桥、桥的MAC地址、桥ID、端口ID。

- 桥（Bridge）。

因为性能方面的限制等因素，早期的交换机一般只有两个转发端口（如果端口多了，交换的转发速度就会慢得无法接受），所以那时的交换机常常被称为“网桥”，或简称“桥”。在IEEE的术语中，“桥”这个术语一直沿用至今，但并不只是指只有两个转发端口的交换机，而是泛指具有任意多端口的交换机。目

前，“桥”和“交换机”这两个术语是完全混用的，本书也采用了这一混用习惯。

- 桥的MAC地址（Bridge MAC Address）。

我们知道，一个桥有多个转发端口，每个端口有一个MAC地址。通常，我们把端口编号最小的那个端口的MAC地址作为整个桥的MAC地址。

- 桥ID（Bridge Identifier，BID）。

如图7-7所示，一个桥（交换机）的桥ID由两部分组成，前面的2字节是这个桥的桥优先级，后面的6字节是这个桥的MAC地址。桥优先级的值可以人为设定，默认值为0x8000（相当于十进制的32768）。

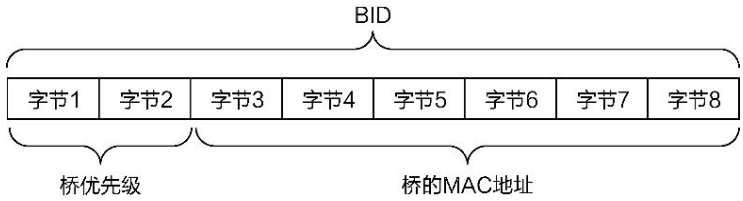


图7-7　BID的组成

- 端口ID（Port Identifier，PID）。

桥（交换机）的端口ID的定义方法有很多种，图7-8给出了其中的两种定义。在第一种定义中，端口ID由2字节组成，第一个字节是该端口的端口优先级，后一个字节是该端口的端口编号。在第二种定义中，端口ID由16比特组成，前4比特是该端口的端口优先级，后12比特是该端口的端口编号。端口优先级的值是可以人为设定的。不同的设备商所采用的PID的定义方法可能不同。

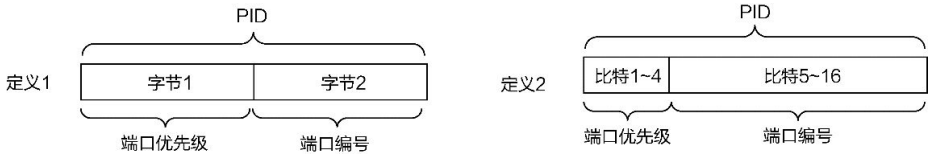


图7-8　PID的组成

7.3.3　生成树协议基本概念和工作原理

生成树协议的基本原理，就是在具有物理环路的交换网络中，交换机通过运行STP自动生成没有环路的网络拓扑。

STP的任务是找到网络中的所有链路，并关闭所有冗余的链路，这样就可以防止网络环路的产生。为了达到这个目的，STP首先需要选举一个根桥（根交换机），由根桥负责决定网络拓扑。一旦所有的交换机都同意将某台交换机选举为根桥，就必须为其余的交换机选定唯一的根端口，还必须为两台交换机之间的每一条链路两端连接的端口（一根网线就是一条链路）选定一个指定端口。既不是根端口也不是指定端口的端口就成为了备用端口，备用端口不转发计算机通信的帧，从而阻断环路。

下面将以图7-9所示的网络拓扑为例讲解生成树的工作过程，分为以下4个步骤。

（1）选举根桥（root bridge）。

（2）为非根桥交换机选定根端口（Root Port，RP）。

（3）为每条链路两端连接的端口选定一个指定端口（Designated Port，DP）。

（4）阻塞备用端口（Alternate Port，AP）。

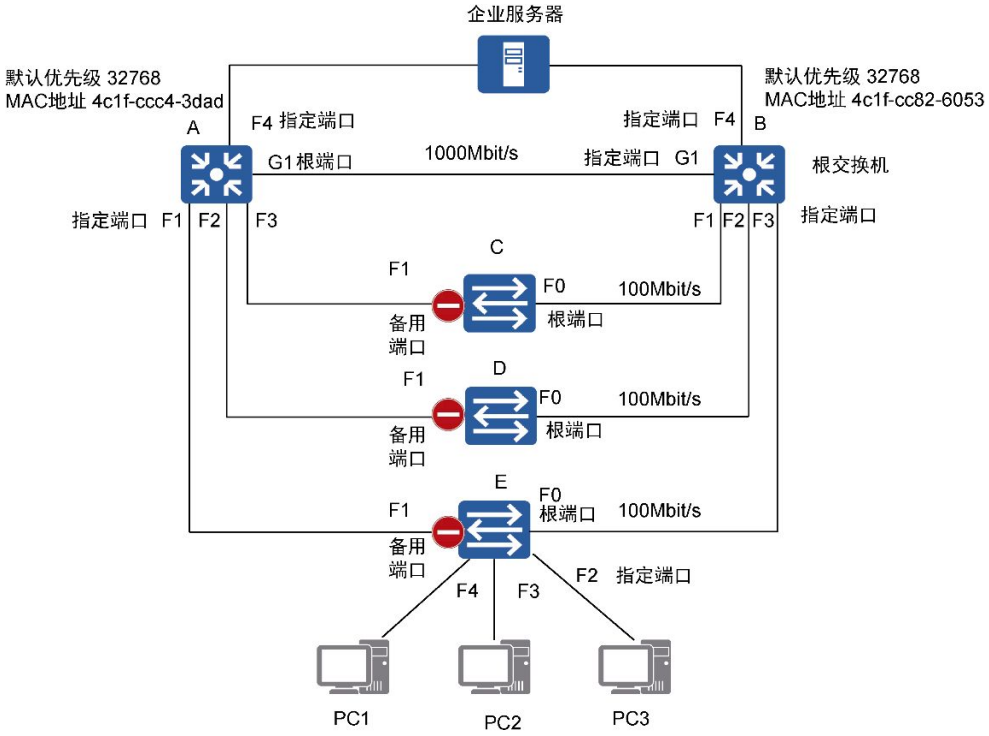


图7-9　生成树的工作过程

1. 选举根桥

根桥是STP树的根节点。要生成一棵STP树，首先要确定出一个根桥。根桥是整个交换网络的逻辑中心，但不一定是它的物理中心。当网络的拓扑发生变化时，根桥也可能会发生变化。

运行STP的交换机（简称为STP交换机）会相互交换STP协议帧，这些协议帧的载荷数据被称为BPDU（Bridge Protocol Data Unit，网桥协议数据单元）。虽然BPDU是STP协议帧的载荷数据，但它并非网络层的数据单元。BPDU的产生者、接收者、处理者都是STP交换机本身，而非终端计算机。BPDU中包含了与STP相关的所有信息（后续会对BPDU进行专门的讲解），其中就有BID。

STP交换机初始启动之后，都会认为自己是根桥，并在发送给别的交换机的BPDU中宣告自己是根桥。当交换机从网络中收到其他设备发送过来的BPDU时，会

比较BPDU指定的根桥BID和自己的BID。交换机不断地交互BPDU，同时与BID进行比较，直至最终选举出一台BID最小的交换机作为根桥。

图7-9所示的网络中有A、B、C、D、E这5台交换机，BID最小的将被选举为根桥。

默认每隔2s发送一次BPDU。在本例中，交换机A和交换机B的优先级相同，交换机B的MAC地址为4c1f-cc82-6053，比交换机A的MAC地址4c1f-ccc4-3dad小，交换机B的就更有可能成为根桥。此外可以通过更改交换机的优先级来指定成为根桥的首选交换机和备用交换机。通常我们会事先指定性能较好、距离网络中心较近的交换机作为根桥。在本示例中显然让交换机A和交换机B成为根桥的首选和备用交换机最佳。

2. 选定根端口

根桥确定后，其他没有成为根桥的交换机都被称为非根桥。非根桥设备上可能会有多个端口与网络相连，为了保证从某台非根桥设备到根桥设备的工作路径是最优且唯一的，就必须从该非根桥设备的端口中确定一个被称为“根端口”的端口，由根端口来作为该非根桥设备与根桥设备之间进行报文交互的端口。一台非根桥设备上最多只能有一个根端口。

STP把根路径开销作为确定根端口的一个重要依据。一个运行STP的网络中，我们将某个交换机的端口到根桥的累计路径开销（即从该端口到根桥所经过的所有链路的路径开销的和）称为这个端口的根路径开销（Root Path Cost，RPC）。链路的路径开销（path cost）与端口速率有关，端口速率越大，则路径开销越小。端口速率与路径开销的对应关系可参考表7-1。

表7-1　端口速率和路径开销的对应关系

端 口 速 率	路径开销（IEEE 802.1t标准）
10Mbit/s	2000000
100Mbit/s	200000
1000Mbit/s	20000
10Gbit/s	2000

在本例中，确定了交换机B为根桥后，交换机A、C、D和E就是非根桥，每个非根桥要选择一个到达根桥最近（累计开销最小）的端口作为根端口。对于A的G1接口，C、D、E的F0接口成为这些交换机的根端口。

如图7-10所示，S1为根桥，假设S4到根桥的路径1的开销和路径2的开销相同，则S4会对上行设备S2和S3的网桥ID进行比较，如果S2的网桥ID小于S3的网桥ID，那么S4会将自己的G0/0/1确定为自己的根端口；如果S3的网桥ID小于S2的网桥ID，那么S4会将自己的G0/0/2确定为自己的根端口。

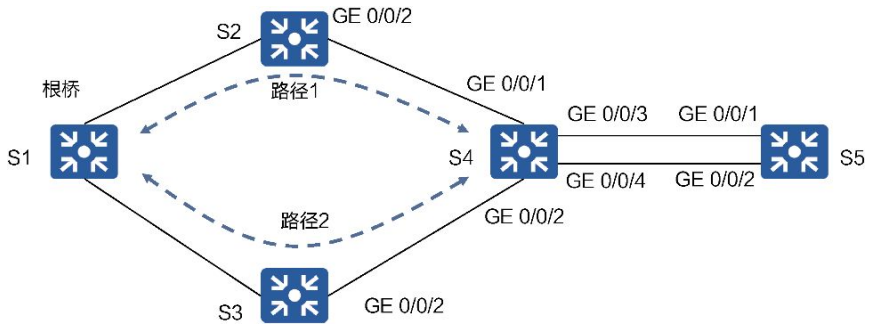


图7-10　确定根端口

对于S5而言，假设其GE 0/0/1端口的RPC与GE0/0/2的端口RPC相同，由于这两个接口的上行设备同为S4，所以S5还会对S4的GE0/0/3和GE0/0/4端口的PID进

行比较。如果S4的GE0/0/3端口PID小于GE0/0/4的PID，则S5会将自己的GE0/0/1作为根端口；如果S4的GE0/0/4端口PID小于GE0/0/3的PID，则S5会将自己的GE0/0/2作为根端口。

3. 选定指定端口

根端口保证了交换机与根桥之间工作路径的唯一性和最优性。为了防止工作环路存在，连接交换机的每根网线两端连接的端口要确定一个指定端口。当一个网段有两条及两条以上的路径通往根桥时（该网段连接了不同的交换机，或者该网段连接了同台交换机的不同端ID），与该网段相连的交换机（可能不止一台）就必须确定出一个唯一的指定端口。

指定端口也是通过比较RPC来确定的。RPC较小的端口将成为指定端口，如果RPC相同，则先比较BID，如果BID相同再比较设备的PID，值小的那个接口成为指定端口。

如图7-11所示，假定S1已被选举为根桥，并且假定各链路的开销均相等。显然，S3的GE0/0/1端口的RPC小于S3的GE0/0/2端口的RPC，所以S3将自己的GE0/0/1端口确定为自己的根端口。类似地，S2的GE0/0/1端口的RPC小于S2的GE0/0/2端口的RPC，所以S2将自己的GE0/0/1端口确定为自己的根端口。

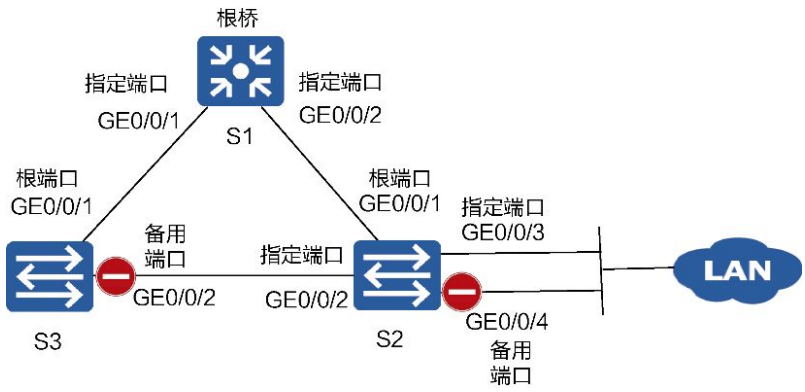


图7-11　确定指定端口

对于S3的GE0/0/2和S2的GE0/0/2之间的网段来说，S3的GE0/0/2端口的RPC是与S2的GE0/0/2端口的RPC相等的，所以需要比较S3的BID和S2的BID。假定S2的BID小于S3的BID，则S2的GE0/0/2端口将被确定为S3的GE0/0/3和S2的GE0/0/2之间的网段的指定端口。

对于网段LAN来说，与之相连的交换机只有S2。在这种情况下，就需要比较S2的GE0/0/3端口的PID和GE0/0/4端口的PID。假定GE0/0/3端口的PID小于GE0/0/4端口的PID，则S2的GE0/0/3端口将被确定为网段LAN的指定端口。

在图7-9所示的网络中，由于交换机A和B之间的连接带宽为1000Mbit/s，因此交换机A的F1、F2、F3端口比交换机C、D和E的F1端口的RPC小，因此交换机A的F1、F2和F3端口成为指定端口。根桥的所有端口都是指定端口，E交换机连接计算机的F2、F3、F4端口为指定端口。

4. 阻塞备用端口

确定了根端口和指定端口后，剩下的端口就是非指定端口和非根端口，这些端口统称为备用端口。STP会对这些备用端口进行逻辑阻塞。所谓逻辑阻塞，是指这些备用端口不能转发由终端计算机产生并发送的帧，这些帧也被称为用户数据帧。不过，备用端口可以接收并处理STP协议帧，根端口和指定端口既可以发送和接收STP协议帧，又可以转发用户数据帧。

一旦备用端口被逻辑阻塞后，STP树（无环工作拓扑）的生成过程便已完成。

7.3.4 生成树的端口状态

- 对于运行STP的网桥或交换机来说，其端口状态会在下列5种状态之间转变。
- 阻塞（Blocking）：被阻塞的端口将不能转发帧，它只监听 BPDU。设置阻塞状态的意图是防止使用有环路的路径。当交换机加电时，默认情况下所有

的端口都处于阻塞状态。

- 侦听（Listening）：端口都会侦听BPDU，以确信在传送数据帧之前，网络上没有环路产生。处于侦听状态的端口没有形成 MAC地址表时，就准备转发数据帧。
- 学习（Learning）：交换机端口侦听 BPDU，并学习交换式网络中的所有路径。处在学习状态的端口形成MAC地址表，但不能转发数据帧。转发延迟是指将端口从侦听状态转换到学习状态所花费的时间，默认设置为15s，可以执行命令display spanning- tree来查看。
- 转发（Forwarding）：在桥接的端口上，处在转发状态的端口发送并接收所有的数据帧。如果在学习状态结束时，端口仍然是指定端口或根端口，它就会进入转发状态。
- 禁用（Disabled）：从管理上讲，处于禁用状态的端口不能参与帧的转发或形成STP。在禁用状态下，端口实质上是不工作的。

在大多数情况下，交换机端口都处在阻塞或转发状态。转发端口是指到根桥开销最低的端口，但如果网络的拓扑发生改变（可能是链路失效了，或者有人添加了一台新的交换机），交换机上的端口就会处于侦听或学习状态。

正如前面提到的，阻塞端口是一种防止网络环路的策略。一旦交换机决定了到根桥的最佳路径，所有其他的端口就将处于阻塞状态。被阻塞的端口仍然能接收BPDU，它们只是不能发送任何帧。

7.3.5 STP的缺点和RSTP概述

在STP网络中，如果新增或减少交换机，或者更改了交换机的网桥优先级，或者某条链路失效，那么STP就有可能重新选定根桥，为非根桥重新选定根端口，并为每条链路重新选定指定端口。那些处于阻塞状态的端口有可能变成转发端口，这个过程需要十几秒的时间（这段时间又称为收敛时间），在此期间网络会中断。为了缩短收敛时间，IEEE 802.1w定义了快连生成树协议（Rapid Spanning Tree Protocol，RSTP），RSTP在STP的基础上进行了许多改进，使收敛时间大大减少，一般只需要几秒。在现实网络中STP几乎已经停止使用，取而

代之的是RSTP，RSTP最重要的一个改进就是端口状态只有3种：放弃、学习和转发。

7.3.6　查看和配置STP

用3台交换机S1、S2和S3组建企业局域网，网络拓扑如图7-12所示，下面的操作可实现以下功能。

- 启用STP。
- 确定根桥。
- 查看端口状态。
- 配置STP模式为RSTP。
- 指定根桥和备用的根桥。
- 配置边缘端口。

在S1上显示生成树运行状态。

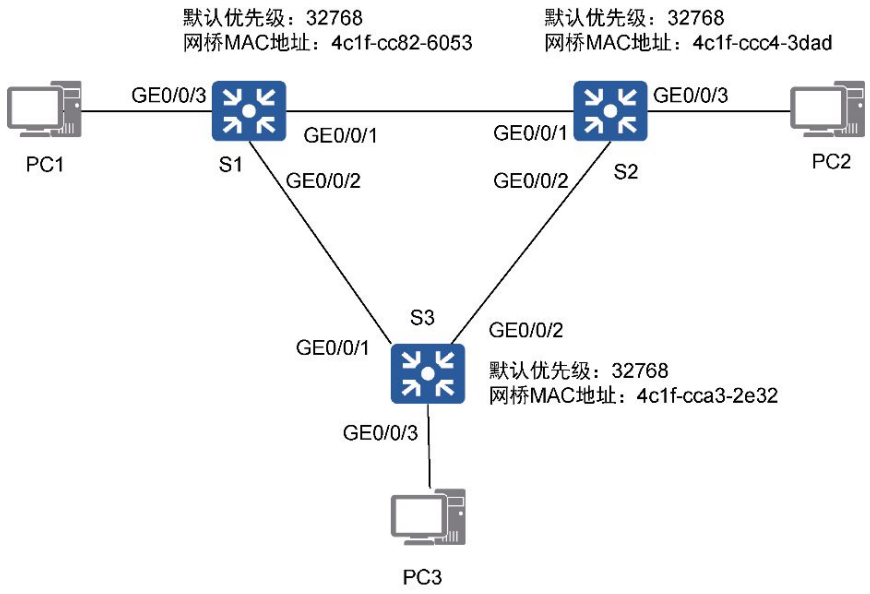


图7-12　生成树实验网络拓扑

```
[S1]display stp
-------[CIST Global Info][Mode MSTP]-------      --全局设置，STP模式默认为MSTP
CIST Bridge      :32768.4c1f-cc82-6053           --交换机S1的ID，32768是优先级
```

```
Config Times    :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times    :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC  :32768.4c1f-cc82-6053 / 0       --根交换机ID，S1就是根交换机
CIST RegRoot/IRPC   :32768.4c1f-cc82-6053 / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :7
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:3m:23s
Number of TC        :8
Last TC occurred    :GigabitEthernet0/0/1
----[Port1(GigabitEthernet0/0/1)][FORWARDING] - -  --端口GigabitEthernet 0/0/1
处于转发状态
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128                            --端口优先级，默认为128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :32768.4c1f-cc82-6053 / 128.1
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :1
 TC or TCN received  :0
 BPDU Sent           :96
     TCN: 0, Config: 0, RST: 0, MST: 96
 BPDU Received       :1
     TCN: 0, Config: 0, RST: 0, MST: 1
    ……
```

显示STP端口状态。

```
[S1]display stp brief
 MSTID  Port              Role  STP  State  Protection
  0    GigabitEthernet0/0/1    DESI  FORWARDING     NONE      --指定端口，转发状
态
  0    GigabitEthernet0/0/2    DESI  FORWARDING     NONE      --指定端口，转发状
态
  0    GigabitEthernet0/0/3    DESI  FORWARDING     NONE      --指定端口，转发状
态
```

根交换机上的所有端口都是指定端口（DESI），其中GigabitEthernet 0/0/3端口连接计算机，也会参与到生成树协议中。

执行以下命令关闭生成树协议。

```
[S1]stp disable
```

执行以下命令启用生成树协议。华为交换机STP默认已经启用。

```
[S1]stp enable
```

配置STP模式为RSTP。

```
[S1]stp mode ?          --查看生成树有几种模式
  mstp  Multiple Spanning Tree Protocol (MSTP) mode
  rstp  Rapid Spanning Tree Protocol (RSTP) mode
  stp   Spanning Tree Protocol (STP) mode
[S1]stp mode rstp       --设置STP模式为RSTP
```

虽然STP会自动选举根桥，但一般情况下，网络管理员会事先指定性能较好、距离网络中心较近的交换机作为根桥。可以更改交换机的优先级来指定根桥和备用的根桥。

下面更改交换机S2的优先级，让其优先成为根桥；更改S1的优先级，让其成为备用根桥。

```
[S2]stp priority ?
  INTEGER<0-61440>  Bridge priority, in steps of 4096 --优先级取值范围，取值是
4096的倍数
[S2]stp priority 0                                    --优先级设置为0
[S1]stp priority 4096                                 --优先级设置为4096
```

也可以使用以下命令将S2的优先级设置为0。

```
[S2]stp root primary
```

也可以使用以下命令将S1的优先级设置为4096。

```
[S1]stp root secondary
```

在S2上查看STP信息。

```
 [S2]display stp
-------[CIST Global Info][Mode RSTP]-------        --STP模式为RSTP
```

```
CIST Bridge    :0    .4c1f-ccc4-3dad               --优先级为0
Config Times   :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times   :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC    :0    .4c1f-ccc4-3dad / 0
CIST RegRoot/IRPC :0    .4c1f-ccc4-3dad / 0
…
```

在S3上查看STP摘要信息。

```
<S3>display stp brief
 MSTID  Port              Role  STP State   Protection
  0  GigabitEthernet0/0/1     ALTE  DISCARDING     NONE
  0  GigabitEthernet0/0/2     ROOT  FORWARDING     NONE
  0  GigabitEthernet0/0/3     DESI  FORWARDING     NONE
```

可以看到GigabitEthernet 0/0/1为备用端口，状态为DISCARDING（丢弃）。GigabitEthernet 0/0/2为根端口，状态为FORWARDING（转发）。GigabitEthernet 0/0/3为指定端口，状态为FORWARDING（转发）。

ROOT表示端口角色为根端口。

ALTE是英文单词Alternative的缩写，端口角色为备用端口。

DESI是英文单词Designation的缩写，端口角色为指定端口。

生成树的计算主要发生在交换机互连的链路上，而连接PC的端口没有必要参与生成树计算。为了优化网络，并降低生成树计算机对终端设备的影响，可把交换机连接PC的端口配置成边缘端口。

以下操作禁止启用交换机的端口GigabitEthernet 0/0/3，可以看到端口的初始状态为丢弃；15s后，端口进入学习状态；30s后才最终进入转发状态。

```
[S3]display stp brief
 MSTID  Port                Role  STP State  Protection
  0  GigabitEthernet0/0/1     ALTE   DISCARDING     NONE
  0  GigabitEthernet0/0/2     ROOT   FORWARDING     NONE
  0  GigabitEthernet0/0/3     DESI   FORWARDING     NONE   --处于转发状态
[S3]interface GigabitEthernet 0/0/3
[S3-GigabitEthernet0/0/3]shutdown                          --关闭端口
```

```
[S3-GigabitEthernet0/0/3]undo shutdown                    --启用端口
<S3>display stp brief
 MSTID  Port                Role  STP State   Protection
  0  GigabitEthernet0/0/1     ALTE    DISCARDING     NONE
  0  GigabitEthernet0/0/2     ROOT    FORWARDING     NONE
  0  GigabitEthernet0/0/3     DESI    DISCARDING     NONE  --初始状态
```

7.4 VLAN

7.4.1 什么是VLAN

VLAN（Virtual Local Area Network）的中文名为“虚拟局域网”。

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，这使管理员可以根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域 。每一个VLAN都包含一组有着相同需求的计算机工作站 ，它们相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN是一种比较新的技术，工作在OSI参考模型的第2层和第3层，一个VLAN就是一个广播域，VLAN之间的通信是通过第3层的路由器来完成的。

如图7-13所示，公司在办公大楼的第一层、第二层和第三层部署了交换机，这3台交换机均为接入层交换机，通过汇聚层交换机进行连接。公司的销售部、研发部和财务部的计算机在每一层都有。从安全和控制网络广播方面考虑，可以为每一个部门创建一个VLAN。在交换机的不同的VLAN上使用数字对其进行标识，可以将销售部的计算机指定到VLAN 1，为研发部创建VLAN 2，为财务部创建VLAN 3。

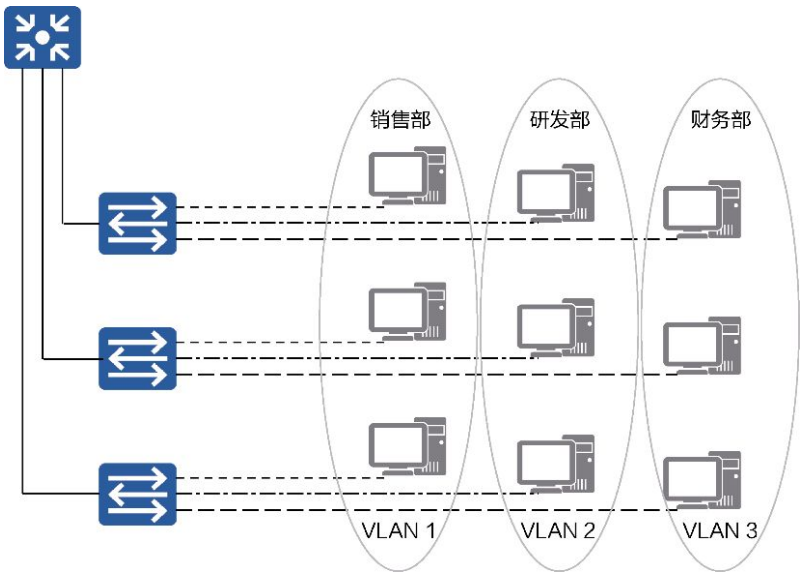


图7-13　VLAN示意图

一个VLAN就是一个广播域，同一个VLAN中的计算机IP地址在同一个网段。

VLAN的优势如下。

- 广播风暴防范。

限制网络上的广播，将网络划分为多个VLAN可减少参与广播风暴的设备数量。VLAN分段可以防止广播风暴波及整个网络。VLAN可以提供防火墙建立的机制，防止交换网络的过量广播。使用VLAN可以将交换端口或计算机指定到某一个特定的VLAN，该VLAN可以在一个交换机中，也可跨多个交换机，在一个VLAN中的广播不会发送到VLAN之外。这样可以把广播控制在一个VLAN内，减少广播造成的影响。

- 安全。

增强局域网的安全性，含有敏感数据的用户组可与网络的其余部分隔离，从而降低泄露机密信息的可能性。不同VLAN内的报文在传输时是相互隔离的，即一个VLAN内的用户不能和其他VLAN内的用户直接通信。如果不同VLAN要进行通信，则需要通过路由器或三层交换机等三层设备。

- 成本降低。

成本高昂的网络升级需求减少，现有带宽和上行链路的利用率更高，从而可节约成本。

- 性能提高。

将第二层平面网络划分为多个逻辑工作组（广播域）可以减少网络上不必要的流量并提高性能。

- 提高人员工作效率。

VLAN为网络管理带来了方便，因为有相似网络需求的用户将共享同一个VLAN。

7.4.2　理解VLAN

交换机的所有端口默认都属于VLAN 1，VLAN 1是默认的VLAN，不能删除。如图7-14所示，交换机S1的所有端口都在VLAN 1中，进入交换机端口的帧自动加上端口所属VLAN的标记，出交换机端口则会去掉VLAN标记。在图7-14中，计算机A给计算机D发送一个帧，帧进入F0端口，加上VLAN 1的标记，出F3端口，去掉VLAN 1的标记。对于通信的计算机A和D而言，这个过程是透明的。如果计算机A发送一个广播帧，该帧会加上VLAN 1的标记，并转发到VLAN 1的所有端口。

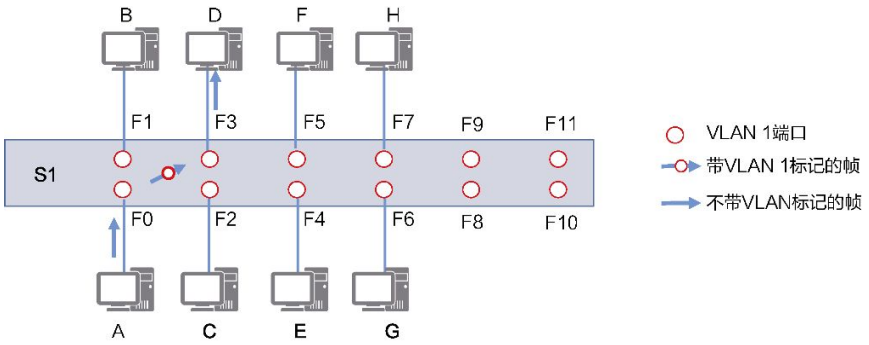


图7-14　交换机端口默认属于VLAN 1

假如交换机S1连接了两个部门的计算机，A、B、C、D是销售部门的计算机，E、F、G、H是研发部门的计算机。为了安全考虑，将销售部门的计算机指定到VLAN 1，将研发部门的计算机指定到VLAN 2。如图7-15 所示，计算机E给计算机H发送一个帧，进入F8端口，该帧加上了VLAN 2的标记，从F11端口出去，去掉了VLAN 2的标记。计算机发送和接收的帧不带VLAN标记。

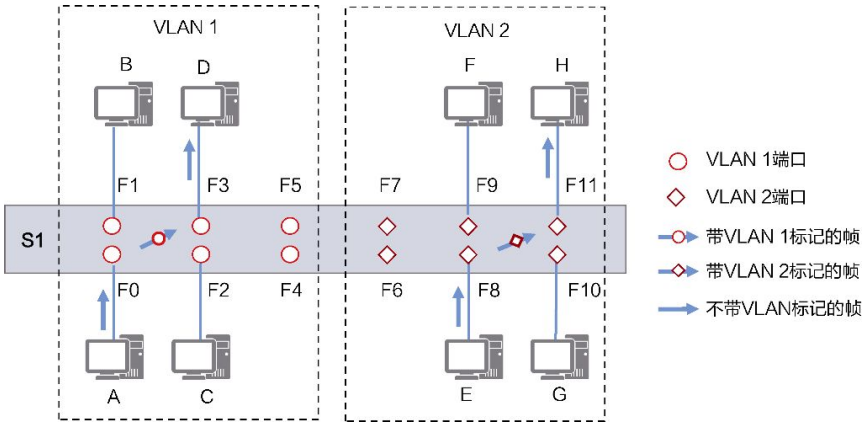


图7-15　交换机上同一VLAN的通信过程

交换机S1划分了两个VLAN，等价于把该交换机逻辑上分成了两个独立的交换机S1-VLAN1和S1-VLAN2，等价图见图7-16。看到这幅等价图，你就知道，不同VLAN的计算机即便IP地址设置成一个网段，也不能通信了。要想实现VLAN间通信，必须经过路由器（三层设备）转发，这就要求不同VLAN分配不同网段的IP地址，图7-16中S1-VLAN 1分配的网段是192.168.1.0/24，S1-VLAN 2分配的网段是192.168.2.0/24。图7-16添加了一个路由器来展示VLAN间的通信过程，路由器的F0端口连接S1-VLAN 1的F5端口，F1端口连接S1-VLAN 2的F7端口。图7-16标记了计算机C给计算机E发送数据包，帧进出交换机端口，以及VLAN标记的变化。

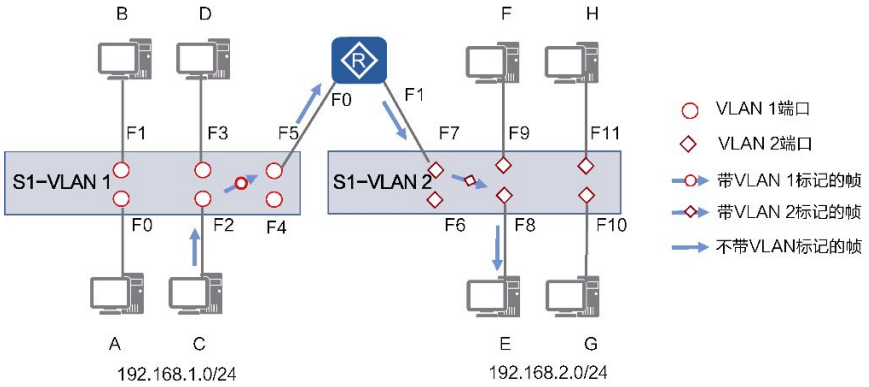


图7-16　VLAN等价图

7.4.3　跨交换机VLAN

前面讲了在一台交换机上可以创建多个VLAN，有时候同一个部门的计算机接到不同的交换机，也要把它们划分到同一个VLAN，这就是跨交换机VLAN。

如图7-17所示，网络中有两台交换机S1和S2，计算机A、B、C、D属于销售部门，计算机E、F、G、H属于研发部门。按部门划分VLAN，销售部门为VLAN 1，研发部门为VLAN 2。为了让S1的VLAN 1和S2的VLAN 1能够通信，需要对两台交换机的VLAN 1端口进行连接，这样计算机A、B、C、D就属于同一个VLAN，VLAN 1跨两台交换机。同样对两台交换机上的VLAN 2端口进行连接，VLAN 2也跨两台交换机。注意观察，计算机D与计算机C通信时帧的VLAN标记变化。

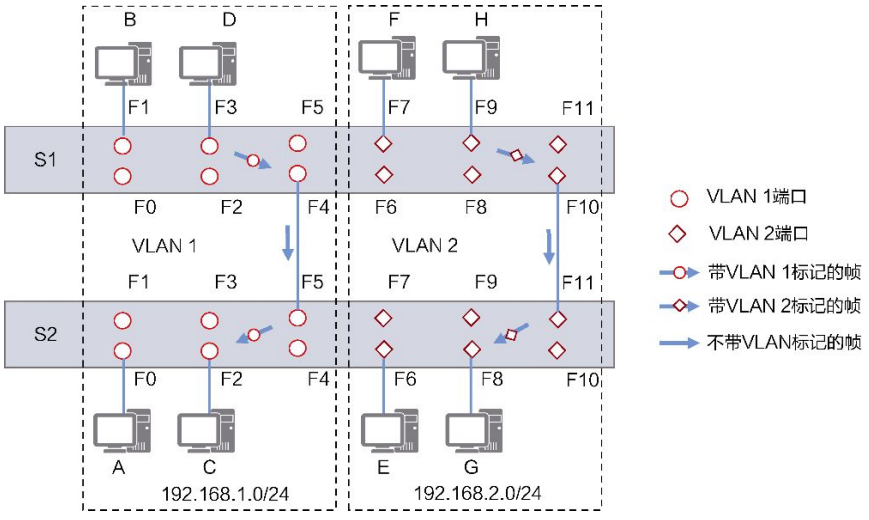


图7-17　跨交换机VLAN

通过图7-17，大家能够很容易地理解跨交换机VLAN如何实现。上面给大家展示了两个跨交换机的VLAN，每个VLAN使用单独的一根网线进行连接。跨交换机的多个VLAN也可以共用同一根网线，这根网线就称为干道链路，干道链路连接的交换机端口就称为干道端口，如图7-18所示。

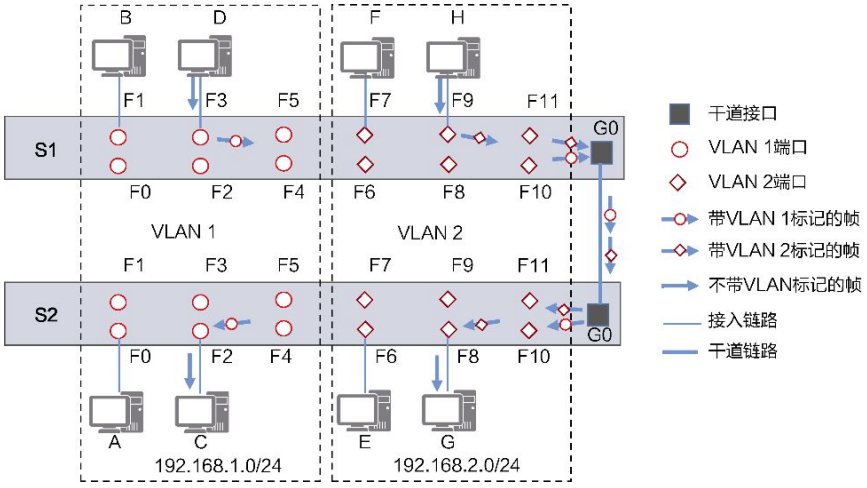


图7-18　干道链路的帧有VLAN标记

在以上网络中，计算机连接交换机的链路称为接入（Access）链路。允许多个VLAN的帧通过的交换机之间的链路称为干道（Trunk）链路。Access链路上的帧不带VLAN标记（Untagged帧），Trunk链路上的帧带有VLAN标记（Tagged帧）。通过干道传递帧，VLAN信息不会丢失。比如计算机B发送一个广播帧，该帧通过干道链路传到交换机S2，交换机S2就知道这个广播帧来自VLAN 1，就把该帧转发到VLAN 1的全部端口。

交换机上的端口分为Access端口、Trunk端口和混合（Hybrid）端口。Access端口只能属于一个VLAN，一般用于连接计算机端口；Trunk端口可以允许多个VLAN的帧通过，进出端口的帧带VLAN标记。

两台交换机、三个VLAN，思考一下，由VLAN 1中的计算机A发送的一个广播帧能否发送到VLAN 2和VLAN 3？

由图7-19可以看到计算机A发出的广播帧，从F2端口发送出去就不带VLAN标记，该帧进入S2的F3端口后加了VLAN 2标记，S2就会把该帧转发到所有VLAN 2端口。计算机B能够收到该帧，该帧从S2的F5端口发送出去，去掉VLAN 2标记。S1的F6端口收到该帧，加上VLAN 3标记后，就把该帧转发给所有的VLAN 3端口，计算机C也能收到该帧。

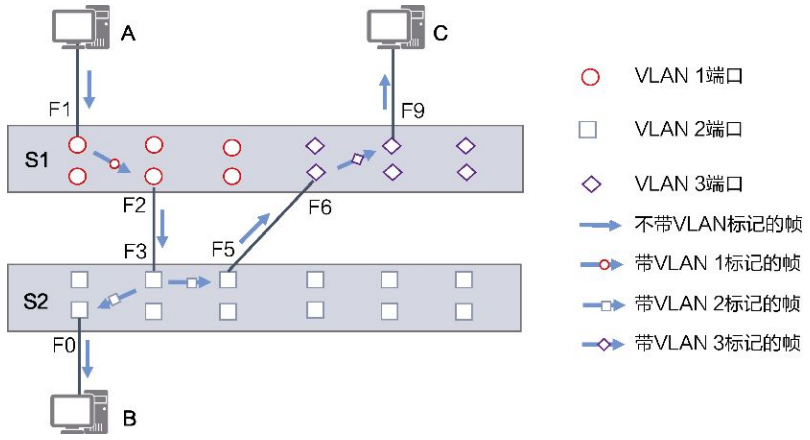


图7-19　交换机之间不要使用Access端口连接

从以上分析可以看到创建了VLAN的交换机，交换机之间的连接最好不要使用Access端口，因为如果连接错误，会造成莫名其妙的网络故障。本来VLAN是隔绝广播帧的，这种连接使得广播帧能够扩散到3个VLAN中。

7.4.4　链路类型和端口类型

一个VLAN帧可能带有Tag（称为Tagged VLAN帧，或简称为Tagged帧），也可能不带Tag（称为Untagged VLAN帧，或简称为Untagged帧）。在谈及VLAN技术时，如果一个帧被交换机划分到VLAN i（i=1，2，3，……，4094），我们就把这个帧简称为一个VLAN i帧。对于带有Tag的VLAN i帧，i其实就是这个帧的Tag中的VID字段的取值。注意，对于Tagged VLAN帧，交换机显然能够从其Tag中的VID值判定出它属于哪个VLAN；对于Untagged VLAN帧（例如终端计算机发出的

帧），交换机需要根据某种原则（比如根据这个帧是从哪个端口进入交换机的）来判定或划分它属于哪个VLAN。

在一个支持VLAN特性的交换网络中，我们把交换机与终端计算机直接相连的链路称为Access链路（Access Link），把Access链路上交换机一侧的端口称为Access端口（Access Port）。同时，我们把交换机之间直接相连的链路称为Trunk链路（Trunk Link），把Trunk链路上两侧的端口称为Trunk端口（Trunk Port）。在一条Access链路上运动的帧只能是（或者说应该是）Untagged帧，并且这些帧只能属于某个特定的VLAN；在一条Trunk链路上运动的帧只能是（或者说应该是）Tagged帧，并且这些帧可以属于不同的VLAN。一个Access端口只能属于某个特定的VLAN，并且只能让属于这个特定VLAN的帧通过；一个Trunk端口可以同时属于多个VLAN，并且可以让属于不同VLAN的帧通过。

每一个交换机的端口（无论是Access端口还是Trunk端口）都应该配置一个PVID（Port VLAN ID)，到达这个端口的Untagged帧将一律被交换机划分到PVID所指代的VLAN。例如，如果一个端口的PVID被配置为5，则所有到达这个端口的Untagged帧都将被认定为是属于VLAN5的帧。在默认情况下，PVID的值为1。

概括地讲，链路（线路）上运动的帧，可能是Tagged帧，也可能是Untagged帧。但一台交换机内部不同端口之间运动的帧则一定是（或者说应该是）Tagged帧。

接下来，我们具体地描述一下Access端口和Trunk端口对于帧的处理和转发规则。

（1）Access端口。

当Access端口从链路（线路）上收到一个Untagged帧后，交换机会在这个帧中添加上VID为PVID的Tag，然后对得到的Tagged帧进行转发操作（泛洪，点到点转发，丢弃）。

当Access端口从链路（线路）上收到一个Tagged帧后，交换机会检查这个帧的Tag中的VID是否与PVID相同。如果相同，则对这个Tagged帧进行转发操作（泛洪，点到点转发，丢弃）；如果不同，则直接丢弃这个Tagged帧。

当一个Tagged帧从本交换机的其他端口到达一个Access端口后，交换机会检查这个帧的Tag中的VID是否与PVID相同。如果相同，则将这个Tagged帧的Tag进行剥离，然后将得到的Untagged帧从链路（线路）上发送出去：如果不同，则直接丢弃这个Tagged帧。

（2）Trunk端口。

对于每一个Trunk端口，除了要配置PVID，还必须配置允许通过的VLAN ID列表。

当Trunk端口从链路（线路）上收到一个Untagged帧后，交换机会在这个帧中添加VID为PVID的Tag，然后查看PVID是否在允许通过的VLAN ID列表中。如果在，则对得到的Tagged帧进行转发操作（泛洪，点到点转发，丢弃）；如果不在，则直接丢弃得到的Tagged帧。

当Trunk端口从链路（线路）上收到一个Tagged帧后，交换机会查看这个帧的Tag中的VID是否在允许通过的VLAN ID列表中。如果在，则对该Tagged帧进行转发操作（泛洪，点到点转发，丢弃）：如果不在，则直接丢弃该Tagged帧。

当一个Tagged帧从本交换机的其他端口到达一个Trunk端口后，如果这个帧的Tag中的VID不在允许通过的VLAN ID列表中，则该Tagged帧会被直接丢弃。

当一个Tagged帧从本交换机的其他端口到达一个Trunk端口后，如果这个帧的Tag中的VID在允许通过的VLAN ID列表中，且VID与PVID相同，则交换机会对这个Tagged帧的Tag进行剥离，然后将得到的Untagged帧从链路（线路）上发送出去。

当一个Tagged帧从本交换机的其他端口到达一个Trunk端口后，如果这个帧的Tag中的VID在允许通过的VLAN ID列表中，但VID与PVID不相同，则交换机不会对这个Tagged帧的Tag进行剥离，而是直接将它从链路（线路）上发送出去。

以上是对Access端口和Trunk端口的工作机制的描述。在实际的VLAN技术实现中，还常常会定义并配置另外一种类型的端口，称为Hybrid端口。工作人员既可以将交换机上与终端计算机相连的端口配置为Hybrid端口，也可以将交换机上与其他交换机相连的端口配置为Hybrid端口。

（3）Hybrid端口。

Hybrid端口除了需要配置PVID，还需要配置两个VLAN ID列表，一个是Untagged VLAN ID列表，另一个是Tagged VLAN ID列表。这两个VLAN ID列表中的所有VLAN的帧都是允许通过这个Hybrid端口的。

当Hybrid端口从链路（线路）上收到一个Untagged帧后，交换机会在这个帧中添加VID为PVID的Tag，然后查看它是否在Untagged VLAN ID列表或Tagged VLANID列表中。如果在，则对得到的Tagged帧进行转发操作（泛洪，点到点转发，丢弃）：如果不在，则直接丢弃得到的Tagged帧。

当Hybrid端口从链路（线路）上收到一个Tagged帧后，交换机会查看这个帧的Tag中的VID是否在Untagged VLAN ID列表或Tagged VLAN ID列表中。如果在，则对该Tagged帧进行转发操作（泛洪，点到点转发，丢弃）；如果不在，则直接丢弃该Tagged帧。

当一个Tagged帧从本交换机的其他端口到达一个Hybrid端口后，如果这个帧的Tag中的VID既不在Untagged VLAN ID列表中，也不在Tagged VLAN ID列表中，则该Tagged帧会被直接丢弃。

当一个Tagged帧从本交换机的其他端口到达一个Hybrid端口后，如果这个帧的Tag中的VID在Untagged VLAN ID列表中，则交换机会对这个Tagged帧的Tag进行剥离，然后将得到的Untagged帧从链路（线路）上发送出去。

当一个Tagged帧从本交换机的其他端口到达一个Hybrid端口后，如果这个帧的Tag中的VID在Tagged VLAN ID列表中，则交换机不会对这个Tagged帧的Tag进行剥离，而是直接将它从链路（线路）上发送出去。

Hybrid端口的工作机制比Trunk端口和Access端口的更为丰富而灵活：Trunk端口和Access端口可以看作Hybrid端口的特例。当Hybrid端口配置中的Untagged VLAN ID列表中有且只有PVID时，Hybrid端口就等效于一个Trunk端口；当Hybrid端口配置中的Untagged VLAN ID列表中有且只有PVID，并且Tagged VLAN ID列表为空时，Hybrid端口就等效于一个Access端口。

7.4.5 VLAN的类型

计算机发送的帧都是不带Tag的。对于一个支持VLAN特性的交换网络来说，当计算机发送的Untagged帧一旦进入交换机，交换机就必须通过某种划分原则把这个帧划分到某个特定的VLAN中。根据划分原则的不同，VLAN便有了不同的类型。

（1）基于端口的VLAN（Port-based VLAN）。

划分原则：将VLAN的编号（VLAN ID）配置影射到交换机的物理端口上。从某一物理端口进入交换机的、由终端计算机发送的Untagged帧都被划分到该端口的VLAN ID所指明的那个VLAN。这种划分原则简单而直观，实现也很容易，并且也比较安全可靠。注意，对于这种类型的VLAN，当计算机接入交换机的端口发生变化时，该计算机发送的帧的VLAN归属可能会发生改变。基于端口的VLAN通常也称为物理层VLAN，或一层VLAN。

（2）基于MAC地址的VLAN（MAC-based VLAN）。

划分原则：交换机内部建立并维护了一个MAC地址与VLAN ID的对应表。当交换机接收到计算机发送的Untagged帧时，交换机将分析帧中的源MAC地址，然后查询MAC地与VLAN ID的对应表，并根据对应关系把这个帧划分到相应的VLAN中。这种划分原则实现起来稍显复杂，但灵活性得到了提高。例如，当计算机接入交换机的端口发生了变化时，该计算机发送的帧的VLAN归属并不会发生改变（因为计算机的MAC地址不会发生变化）。但需要指出的是，这种类型的VLAN的安全性不是很高，因为一些恶意的计算机是很容易伪造自己的MAC地址的。基于MAC地址的VLAN通常也称为二层VLAN。

（3）基于协议的VLAN（Protocol-based VLAN）。

划分原则：交换机根据计算机发送的Untagged帧中的帧类型字段的值来决定帧的VLAN归属。例如，可以将类型值为0x0800的帧划分到一个VLAN，将类型值为0x86dd的帧划分到另一个VLAN；这实际上是将载荷数据为IPv4 Packet的帧和载荷数据为IPv6 Packet的帧分别划分到了不同的VIAN。基于协议的VLAN通常也称为三层VLAN。

以上介绍了3种不同类型的VLAN。从理论上说，VLAN的类型远远不止这些，因为划分VLAN的原则可以是灵活而多变的，并且某一种划分原则还可以是另外若干种划分原则的某种组合。在现实中，究竟该选择什么样的划分原则，需要根据网络的具体需求、实现成本等因素决定。就目前来看，基于端口的VLAN在实际的网络中应用最为广泛。如无特别说明，本书中所提到的VLAN，均是指基于端口的VLAN。

7.4.6　配置基于端口的VLAN

下面就以二层结构的局域网为例创建基于端口的跨交换机的VLAN。

如图7-20所示，网络中有两台接入层交换机LSW2和LSW3、一台汇聚层交换机LSW1；网络中有6台计算机，PC1和PC2在VLAN 1，PC3和PC4在VLAN 2，PC5和PC6在VLAN 3，VLAN1所在的网段是192.168.1.0/24，VLAN2所在的网段是192.168.2.0/24，VLAN3所在的网段是192.168.3.0/24。

我们需要完成以下功能。

（1）每个交换机都创建VLAN1、VLAN2和VLAN3，VLAN1指默认VLAN不需要创建。

（2）将接入层交换机端口Ethernet 0/0/1～Ethernet 0/0/5指定到VLAN 1。

（3）将接入层交换机端口Ethernet 0/0/6～Ethernet 0/0/10指定到VLAN 2。

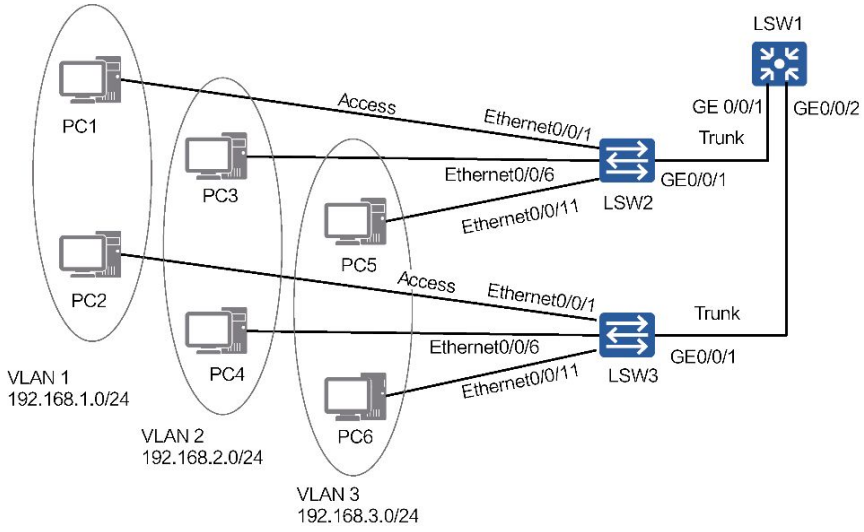


图7-20　跨交换机VLAN

（4）将接入层交换机端口Ethernet 0/0/11～Ethernet 0/0/15指定到VLAN 3。

（5）将连接计算机的端口设置成Access端口。

（6）将交换机之间的连接端口设置成Trunk，允许VLAN 1、VLAN 2、VLAN 3的帧通过。

（7）捕捉、分析干道链路上带VLAN标记的帧。

在这里你要记住将交换机接计算机的端口要设置成Access端口，交换机和交换机连接的端口要设置成Trunk端口。也可以这样记，如果接口需要多个VLAN的帧通过，就需要将其设置成Trunk端口。同时还要记住交换机的这些Trunk端口的PVID要一致。汇聚层交换机虽然没有连接VLAN 2和VLAN 3的计算机，但也需要创建VLAN2和VLAN 3，也就是说网络中的这三台交换机要有相同的VLAN。

在交换机LSW2上创建VLAN。

```
[LSW2]vlan ?
 INTEGER<1-4094>  VLAN ID                          --支持的VLAN数量，最大4094
 batch     Batch process                           --可以批量创建VLAN
[LSW2]vlan 2                                       --创建VLAN 2
[LSW2-vlan2]quit
[LSW2]vlan 3                                       --创建VLAN 3
[LSW2-vlan3]quit
[LSW2]display vlan summary                         --显示VLAN摘要信息
static vlan:
Total 3 static vlan.                               --总共3个VLAN
  1 to 3
dynamic vlan:
Total 0 dynamic vlan.
reserved vlan:
Total 0 reserved vlan.
[LSW2]
```

VLAN 1是默认VLAN，不用创建。

以下命令可批量创建VLAN 4、VLAN 5和VLAN 6。

```
[LSW2]vlan batch 4 5 6
```

以下命令可批量创建VLAN 10～VLAN 20 共11个VLAN。

```
vlan batch 10 to 20
```

以下命令可批量删除VLAN 4、VLAN 5和VLAN 6。

```
[LSW2]undo vlan batch 4 5 6
```

由于要批量设置端口，所以有必要创建端口组以进行批量设置。下面的操作将创建端口组vlan1port，将Ethernet 0/0/1～Ethernet 0/0/5端口设置为Access端口，并将它们指定到VLAN 1。

```
[LSW2]port-group vlan1port
[LSW2-port-group-vlan1port]group-member Ethernet 0/0/1 to Ethernet 0/0/5
[LSW2-port-group-vlan1port]port link-type ?      --查看支持的端口类型
  access   Access port
  dot1q-tunnel  QinQ port
  hybrid   Hybrid port
  trunk    Trunk port
[LSW2-port-group-vlan1port]port link-type access  --将端口设置成Access
[LSW2-port-group-vlan1port]port default vlan 1    --指定到VLAN 1
[LSW2-port-group-vlan1port]quit
```

为VLAN 2创建端口组vlan2port，将Ethernet 0/0/6～Ethernet 0/0/10端口设置为Access端口，并将它们指定到VLAN 2。

```
[LSW2]port-group vlan2port
[LSW2-port-group-vlan2port]group-member Ethernet 0/0/6 to Ethernet 0/0/10
[LSW2-port-group-vlan2port]port link-type access
[LSW2-port-group-vlan2port]port default vlan 2
[LSW2-port-group-vlan2port]quit
```

为VLAN 3创建端口组vlan3port，将Ethernet 0/0/11～Ethernet 0/0/15端口设置为Access端口，并将它们指定到VLAN 3。

```
[LSW2]port-group vlan3port
[LSW2-port-group-vlan3port]group-member Ethernet 0/0/11 to Ethernet 0/0/15
[LSW2-port-group-vlan3port]port link-type access
[LSW2-port-group-vlan3port]port default vlan 3
[LSW2-port-group-vlan3port]quit
```

将GigabitEthernet 0/0/1端口配置为Trunk类型，允许VLAN 1、VLAN 2和VLAN3的帧通过。

```
[LSW2]interface GigabitEthernet 0/0/1
[LSW2-GigabitEthernet0/0/1]port link-type trunk
[LSW2-GigabitEthernet0/0/1]port trunk allow-pass vlan ?
  INTEGER<1-4094>  VLAN ID
  all      All                                  --允许所有VLAN的帧通过
[LSW2-GigabitEthernet0/0/1]port trunk allow-pass vlan 1 2 3 --指定允许通过的
VLAN
```

显示VLAN设置，可以看到端口GE 0/0/1同时属于VLAN 1、VLAN 3和VLAN 3。

```
[LSW2]display vlan
The total number of vlans is : 3               --VLAN数量
--------------------------------------------------------------------------------
---
U: Up;    D: Down;  TG: Tagged;   UT: Untagged; --TG:带VLAN标记。UT：不带VLAN标记
MP: Vlan-mapping;       ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
---

VID  Type    Ports
--------------------------------------------------------------------------------
---
1    common  UT:Eth0/0/1(U)     Eth0/0/2(D)     Eth0/0/3(D)     Eth0/0/4(D)
         Eth0/0/5(D)     Eth0/0/16(D)    Eth0/0/17(D)    Eth0/0/18(D)
         Eth0/0/19(D)    Eth0/0/20(D)    Eth0/0/21(D)    Eth0/0/22(D)
         GE0/0/1(U)      GE0/0/2(D)
2    common  UT:Eth0/0/6(U)     Eth0/0/7(D)     Eth0/0/8(D)     Eth0/0/9(D)
         Eth0/0/10(D)
         TG:GE0/0/1(U)
3    common  UT:Eth0/0/11(U)    Eth0/0/12(D)    Eth0/0/13(D)    Eth0/0/14(D)
         Eth0/0/15(D)
         TG:GE0/0/1(U)

……
```

参照LSW2的配置在LSW3上进行配置，创建VLAN并指定端口类型。

在汇聚层交换机SW1上创建VLAN 2、VLAN 3，并将两个端口类型设置成Trunk，允许VLAN 1、VLAN 2、VLAN 3的帧通过。

```
[LSW1]vlan batch  2 3                                  --批量创建VLAN 2和VLAN 3
[LSW1]interface GigabitEthernet 0/0/1
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 1 2 3
[LSW1-GigabitEthernet0/0/1]quit
[LSW1]interface GigabitEthernet 0/0/2
[LSW1-GigabitEthernet0/0/2]port link-type trunk
[LSW1-GigabitEthernet0/0/2]port trunk allow-pass vlan 1 2 3
[LSW1-GigabitEthernet0/0/2] quit
```

抓包来捕获干道链路的帧，可以看到华为交换机的干道链路帧在数据链路层和网络层之间插入了VLAN标记，使用的是IEEE 802.1Q帧格式。VLAN ID使用12位表示，VLAN ID的取值范围为0～4095，由于0和4095为协议保留取值，因此VLAN ID的有效取值范围为1～4094，图7-21展示的帧是VLAN 2的帧。

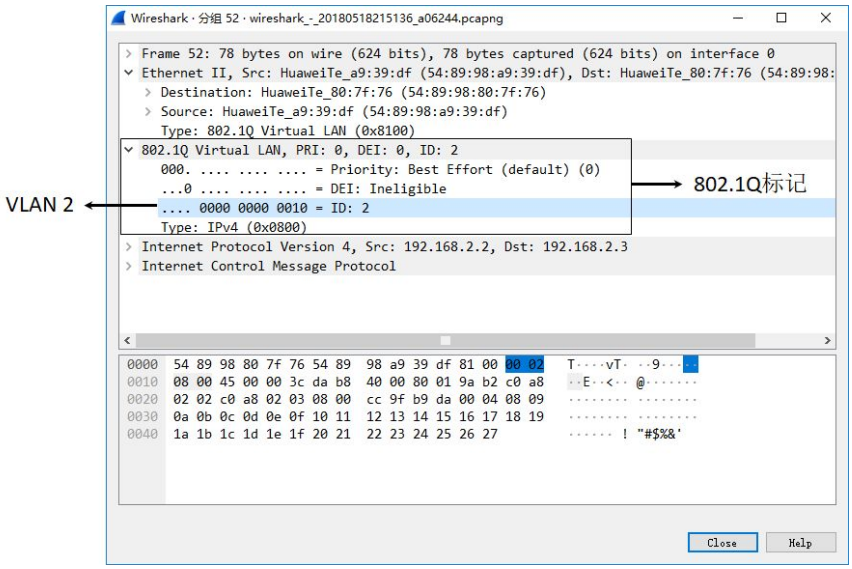


图7-21　带VLAN标记的帧结构

7.4.7　配置基于MAC地址的VLAN

基于MAC地址划分VLAN的方式适用于位置经常移动但网卡不经常更换的小型网络，如移动PC。

如图7-22所示，SwitchA和SwitchB的GE1/0/1接口分别连接两会议室，Laptop1和Laptop2是会议用便携式计算机，在两个会议室间移动使用。Laptop1和Laptop2分别属于两个部门，两个部门间使用VLAN 100和VLAN 200进行隔离。现要求这两台便携式计算机无论在哪个会议室使用，均只能访问自己部门的服务器，即Server1和Server2。Laptop1和Laptop2的MAC地址分别0001-00ef-00c0和0001-00ef-00c1。

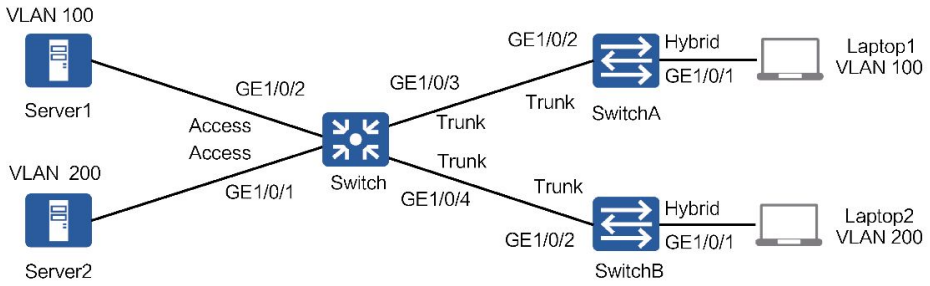


图7-22　基于MAC地址的VLAN

采用如下思路配置基于MAC地址的VLAN。

1．在SwitchA和SwitchB上创建VLAN，并配置Trunk接口和Hybrid接口。

2．在SwitchA和SwitchB基于MAC地址划分VLAN。

3．在Switch上创建VLAN，并配置Trunk和Access接口，保证便携式计算机可以访问服务器。

操作步骤如下。

（1）配置SwitchA。SwitchB的配置与SwitchA相似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200                          --创建VLAN 100和VLAN 200
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk --交换机之间相连的接口类型建议使用trunk。若接口默认类型不是trunk，需要手动配置为trunk
[SwitchA-GigabitEthernet1/0/2] port trunk allow-pass vlan 100 200 --接口GE1/0/2加入VLAN 100和VLAN 200
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] vlan 100
[SwitchA-vlan100] mac-vlan mac-address 0001-00ef-00c0  --MAC地址为0001-00ef-00c0的报文在VLAN 100内转发
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] mac-vlan mac-address 0001-00ef-00c1   --MAC地址为0001-00ef-00c1的报文在VLAN 200内转发
[SwitchA-vlan200] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid   --基于MAC划分VLAN的方式只能应用在类型为hybrid的接口上。V200R005C00及之后版本的默认接口类型不是hybrid，需要手动配置
```

```
[SwitchA-GigabitEthernet1/0/1] port hybrid untagged vlan 100 200   --对VLAN为
100、200的报文，剥掉VLAN Tag
[SwitchA-GigabitEthernet1/0/1] mac-vlan enable  --使能接口的MAC-VLAN功能
[SwitchA-GigabitEthernet1/0/1] quit
```

（2）检查配置结果，在任意视图下执行display mac-vlan mac-address all命令，查看基于MAC地址的VLAN配置。

```
[SwitchA] display mac-vlan mac-address all
------------------------------------------------------
MAC Address        MASK                VLAN    Priority
------------------------------------------------------
0001-00ef-00c0     ffff-ffff-ffff  100     0
0001-00ef-00c1     ffff-ffff-ffff  200     0

Total MAC VLAN address count: 2
```

（3）配置Switch，GE1/0/3和GE1/0/4的配置相同，将其配置成Trunk接口，并允许VLAN 100、VLAN200的帧通过，不再赘述。接口GE1/0/2与GE1/0/1的配置相同，即配置成Access接口，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200                  --创建VLAN 100、VLAN 200
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk allow-pass vlan 100 200  --将接口
GE1/0/2加入VLAN 100和VLAN 200
[Switch-GigabitEthernet1/0/3] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port default vlan 100
[Switch-GigabitEthernet1/0/2] quit
```

7.5　实现VLAN间通信

7.5.1　使用多臂路由器实现VLAN间路由

在交换机上创建多个VLAN，VLAN间的通信可以使用路由器实现。如图7-23所示，两台交换机使用干道链路连接，创建了3个VLAN，路由器的F0、F1和F2端口连接3个VLAN的Access端口，路由器在不同VLAN间转发数据包。路由器的一条物理链路被形象地称为“手臂”，VLAN 1、VLAN 2和VLAN 3中的计算机网关分别是路由器F0、F1、F2接口的地址。图7-23展示了如何使用多臂路由器实现VLAN间路由，另外还展示了VLAN 1中的计算机A与VLAN 3中的计算机L通信的过程，注意观察帧在途经每条链路上的VLAN标记。思考一下计算机H给计算机L发送数据时，帧的路径和经过每条链路时的VLAN标记。

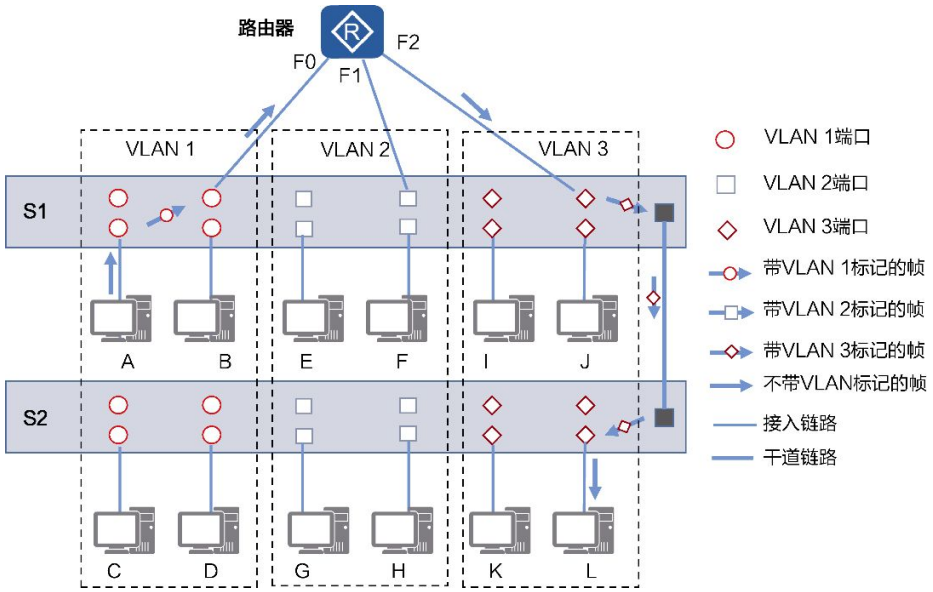


图7-23　使用多臂路由器实现VLAN间路由

将路由器的一个端口连接VLAN的Access端口，一个VLAN需要路由器的一个物理端口，这样增加VLAN时就要考虑路由器的端口是否够用。也可以将路由器的物理端口连接到交换机的干道接口。如图7-24所示，将路由器的物理端口划分成多

个子端口，每个子端口对应一个VLAN，在子端口设置IP地址作为对应VLAN的网关。一个物理端口就可以实现VLAN间路由，这就是使用单臂路由器实现VLAN间路由的过程。图7-24展示了VLAN 1中的计算机A给VLAN 3中的计算机L发送数据包时经过的链路。

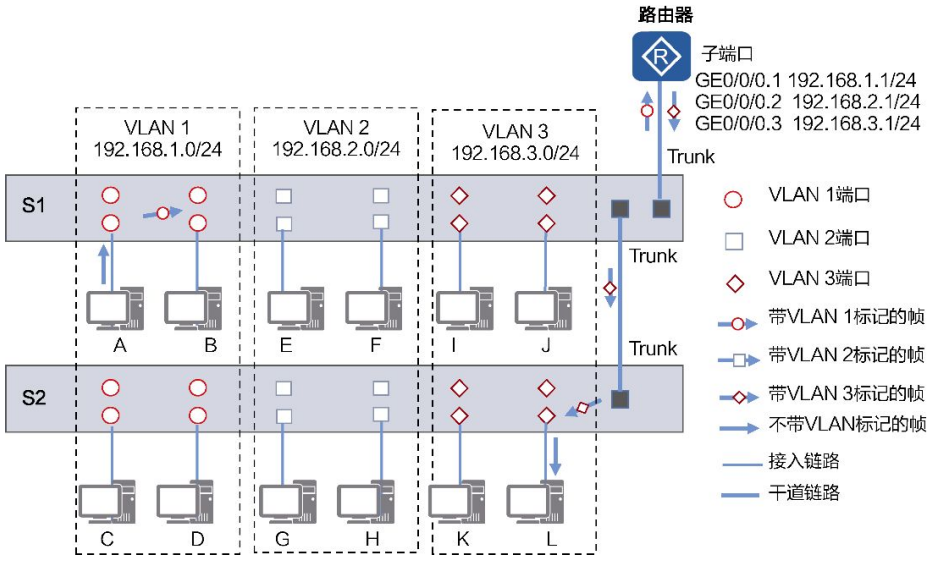


图7-24　使用单臂路由器实现VLAN间路由

7.5.2　使用单臂路由器实现VLAN间路由

如图7-25所示，跨交换机的3个VLAN已经创建完成，在LSW1交换机上连接一个路由器以实现VLAN间通信，需要将LSW1交换机的GE 0/0/3配置成Trunk端口，并允许VLAN 1、VLAN 2和VLAN 3通过。配置AR1路由器的GE 0/0/0物理端口作为VLAN 1的网关，配置GE 0/0/0.2子端口作为VLAN 2的网关，配置GE 0/0/0.3子端口作为VLAN 3的网关。

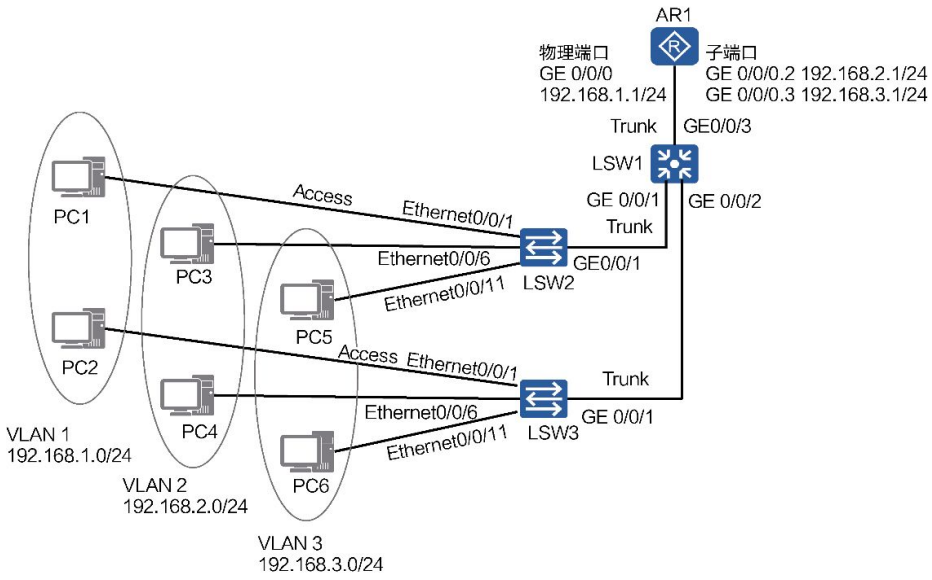


图7-25　配置单臂路由器实现VLAN间路由

配置LSW1上连接路由器的端口GigabitEthernet 0/0/3为Trunk端口，以允许所有VLAN的帧通过。

```
[LSW1]interface GigabitEthernet 0/0/3
[LSW1-GigabitEthernet0/0/3]port link-type trunk
[LSW1-GigabitEthernet0/0/3]port trunk allow-pass vlan all
```

交换机的所有端口都有一个基于端口的VLAN ID（Port-base Vlan ID，PVID），Trunk端口也不例外。显示GigabitEthernet 0/0/3，可以看到GigabitEthernet 0/0/3的PVID是1。该端口发送VLAN 1的帧时会去掉VLAN标记，接收到没有VLAN标记的帧时加上VLAN 1标记。发送和接收其他VLAN的帧时，帧的VLAN标记不变。

```
[LSW1]display interface GigabitEthernet 0/0/3
GigabitEthernet 0/0/3 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :   1, TPID : 8100(Hex), The Maximum Frame Length is 9216
--PVID是1
```

配置AR1路由器的GE 0/0/0端口和子端口。由于连接路由器的交换机的端口PVID是VLAN 1，所以就让物理端口作为VLAN 1的网关，并接收不带VLAN标记的

帧。在物理端口后面加一个数字就代表该物理端口的一个子端口，子端口编号和VLAN编号不要求一致。这里为了好记，子端口编号和VLAN编号设置的一样。

```
[AR1]interface GigabitEthernet 0/0/0              --配置物理端口作为VLAN 1的网关
[AR1-GigabitEthernet0/0/0]ip address 192.168.1.1 24
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface GigabitEthernet 0/0/0.2            --进入子端口
[AR1-GigabitEthernet0/0/0.2]ip address 192.168.2.1 24
[AR1-GigabitEthernet0/0/0.2]dot1q termination vid 2   --指定子端口对应的VLAN
[AR1-GigabitEthernet0/0/0.2]arp broadcast enable      --开启ARP广播功能
[AR1-GigabitEthernet0/0/0.2]quit
[AR1]interface GigabitEthernet 0/0/0.3
[AR1-GigabitEthernet0/0/0.3]ip address 192.168.3.1 24
[AR1-GigabitEthernet0/0/0.3]dot1q termination vid 3   --指定子端口对应的VLAN
[AR1-GigabitEthernet0/0/0.3]arp broadcast enable
[AR1-GigabitEthernet0/0/0.3]quit
```

7.5.3 使用三层交换实现VLAN间路由

三层交换是指在网络交换机中引入路由模块，从而取代传统路由器以实现交换与路由相结合的网络技术。具有三层交换功能的设备是指带有三层路由功能的二层交换机。三层交换机在IP路由的处理上进行了改进，实现了简化的IP转发流程。它利用专用的ASIC芯片实现了硬件的转发，这样绝大多数的报文处理就可以在硬件中实现了，只有极少数报文才需要使用软件转发，这样整个系统的转发性能得以提升千倍，相同性能的设备在成本上也得到大幅下降。

具有三层交换功能的交换机，到底是交换机还是路由器？这对很多读者来说不好理解。大家可以把三层交换机理解成虚拟路由器和交换机的组合。在交换机上有几个VLAN，在虚拟路由器上就有几个虚拟端口（Vlanif）和这几个VLAN相连接。

如图7-26所示，在三层交换机上创建两个VLAN——VLAN 1和VLAN 2，在虚拟路由器上就有两个虚拟端口Vlanif 1和Vlanif 2，这两个虚拟端口相当于分别接入VLAN 1的某个接口和VLAN 2的某个接口。图7-26中的端口F5和Vlanif 1连接，端口F7和Vlanif 2连接。图7-26纯属为了展示，虚拟路由器其实是不可见的，也

不占用交换机的物理端口和Vlanif端口连接。我们能够操作的就是为虚拟端口配置IP地址和子网掩码，让其充当VLAN的网关，让不同VLAN中的计算机能够相互通信。

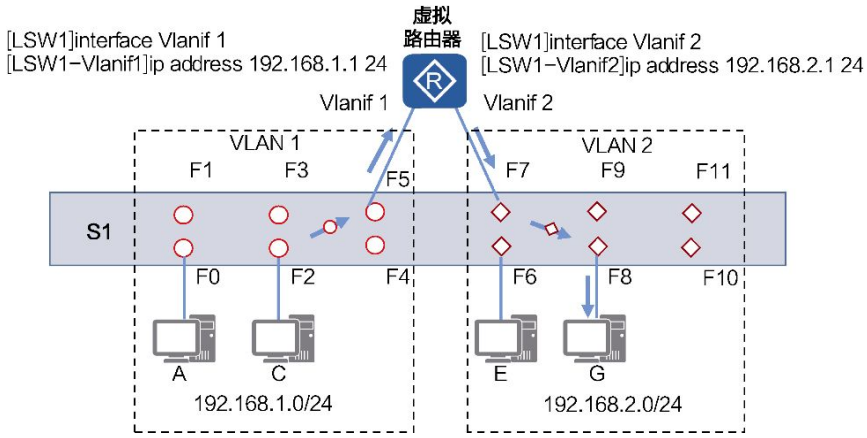


图7-26　三层交换机等价图

7.4.6节的实验只配置了跨交换机的VLAN。继续上面的实验，LSW1是三层交换机，配置LSW1交换机以实现VLAN 1、VLAN 2和VLAN 3的路由。

```
[LSW1]interface Vlanif 1
[LSW1-Vlanif1]ip address 192.168.1.1 24
[LSW1-Vlanif1]quit
[LSW1]interface Vlanif 2
[LSW1-Vlanif2]ip address 192.168.2.1 24
[LSW1-Vlanif2]quit
[LSW1]interface Vlanif 3
[LSW1-Vlanif3]ip address 192.168.3.1 24
[LSW1-Vlanif3]quit
```

输入display ip interface brief显示vlanif接口的IP地址信息以及状态。

```
<LSW1>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 1

Interface                         IP Address/Mask      Physical   Protocol
MEth0/0/1                         unassigned           down         down
```

```
NULL0                          unassigned           up             up(s)
Vlanif1                        192.168.1.1/24       up             up
Vlanif2                        192.168.2.1/24       up             up
Vlanif3                        192.168.3.1/24       up             up
```

7.6 端口隔离

端口隔离可以实现在同一个VLAN内对端口进行逻辑隔离。端口隔离分为L2层隔离和L3层隔离，在这里只讲解和演示L2层隔离。

如图7-27所示，PC1、PC2和PC3在同一个VLAN，不允许它们之间相互通信，但允许它们访问Internet。这就要求设置交换机以实现端口隔离，但不能隔离它们和路由器AR1的GE 0/0/0之间的相互通信。

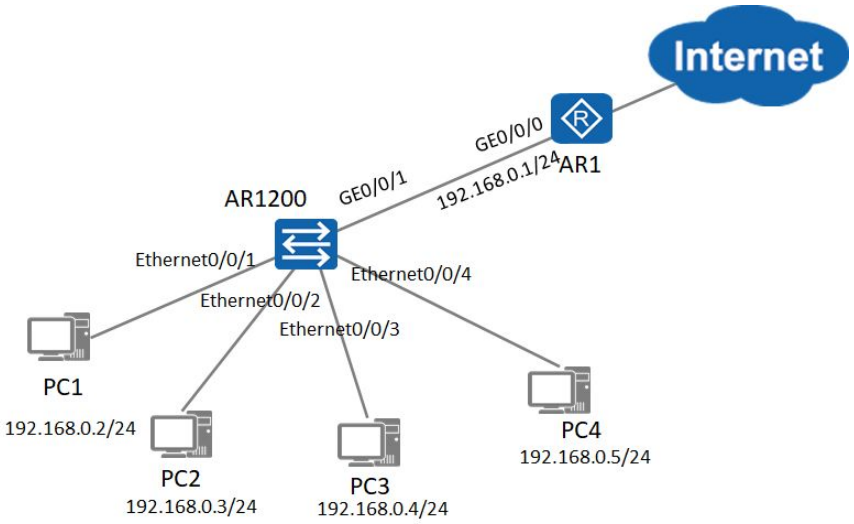


图7-27 端口隔离

下面是交换机S1上的配置步骤，由于要设置多个端口隔离，因此需要定义一个端口组以进行批量设置。

```
[S1]port-isolate mode ?
  all  All
  l2   L2 only
[S1]port-isolate mode l2                                    --启用L2层隔离功能
[S1]port-group vlan1port                                    --定义一个端口组
[S1-port-group-vlan1port]group-member Ethernet 0/0/1 to Ethernet 0/0/4
[S1-port-group-vlan1port]port link-type access
[S1-port-group-vlan1port]port default vlan 1
[S1-port-group-vlan1port]port-isolate enable group ?
  INTEGER<1-64>  Port isolate group-id
[S1-port-group-vlan1port]port-isolate enable group 1    --隔离组内的端口不能相互通信
```

交换机S1的GE 0/0/1不能加入端口隔离组1，处于同一隔离组的各个端口间不能通信。

7.7 链路聚合

7.7.1 链路聚合的基本概念

首先，我们来说明一些常见的说法。读者朋友们可能经常会听到这样一些说法，例如：标准以太口、FE端口、百兆口、GE端口、千兆口，如此等。那么，这些说法究竟是什么意思呢？

其实，这些说法都跟以太网技术的规范有关，特别是跟以太网的信息传输率规范有关。IEEE在制定关于以太网的信息传输率的规范时，信息传输率几乎总是按照十倍关系来递增的。目前，规范化的以太网的信息传输率主要有：10Mbit/s，100Mbit/s，1000Mbit（1Gbit/s），10Gbit/s，100Gbit/s。这种按十倍关系递增的方式既能很好地匹配微电子技术及光学技术的发展，又能控制关于以太网信息传输率规范的散乱性。试想一下，如果IEEE今天推出了一个信息传输率为415Mbit/s的规范，明天又推出了一个信息传输率为624Mbit/s的规范，那么以太网网卡的生产厂家必定会苦不堪言。并且，在实际搭建以太网的时候，以太网链路两端的端口速率匹配问题也会变得非常散乱。

以太网链路的说法是与以太网端口的说法相对应的。例如，如果一条链路两端的端口是GE口，则这条链路就称为一条GE链路；如果一条链路两端的端口是FE口，则这条链路就称为一条FE链路，如此等等。

现在说说什么是链路聚合技术。图7-28展示了某个公司的网络结构；接入层交换机和汇聚层交换机使用GE链路连接。如果打算提高接入层交换机和汇聚层交换机的连接带宽，那么从理论上来讲可以再增加一条GE链路，但STP会阻断其中一条链路的一个端口。

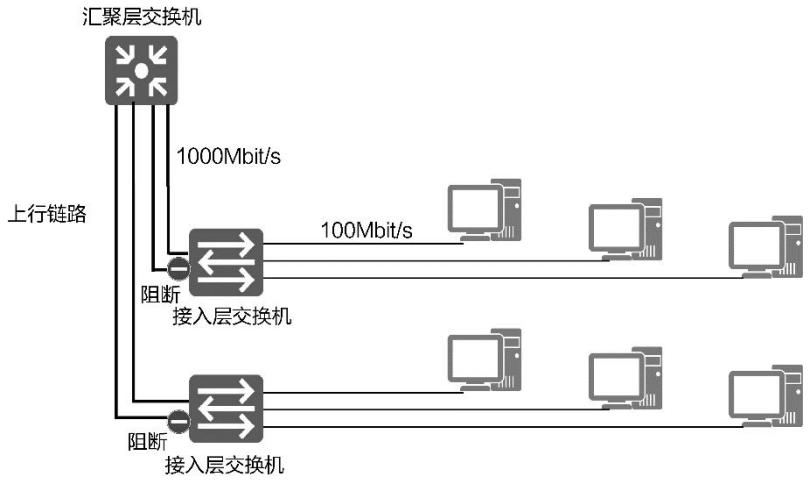


图7-28　在多条上行链路中，STP会阻塞其中一条链路的一个端口

根据扩展链路带宽的需求，需要让链路两端的设备将多条链路视为一条逻辑链路来进行处理，这就是链路聚合技术。如图7-29所示，链路聚合可以实现流量负载均衡和链路冗余，从而节省设备成本。如果两条1000Mbit/s链路构建的2000Mbit/s聚合链路就能满足要求，就不用购买10000Mbit/s接口的设备了。

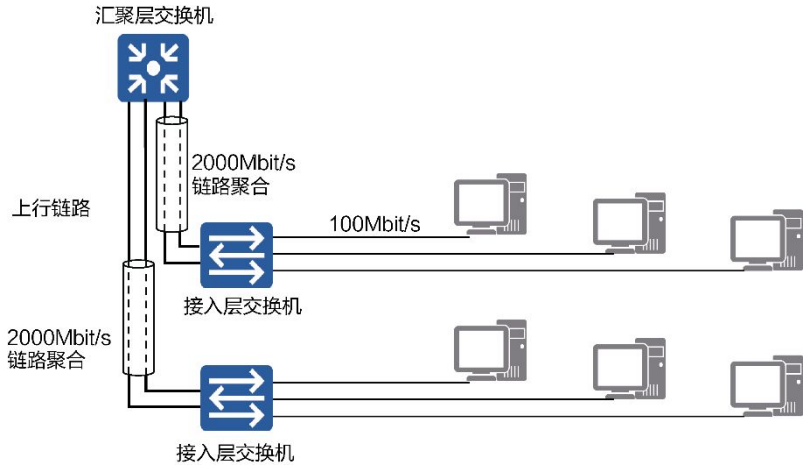


图7-29　链路聚合

7.7.2　链路聚合技术的使用场景

链路聚合也称为链路绑定，英文的说法有：Link Aggregation、Link Trunking、Link Bonding。需要说明的是，这里所说的链路聚合技术，针对的都

是以太网链路。

在7.7.1节里提到的例子中，我们是将链路聚合技术应用在了两台交换机之间。事实上，链路聚合技术还可以应用在交换机与路由器之间，路由器与路由器之间，交换机与服务器之间，路由器与服务器之间，服务器与服务器之间，如图7-30所示。注意，从理论上讲，个人计算机（PC）也是可以实现链路聚合的，但实际上考虑到成本等因素，没人会在现实中去真正实现。另外，从原理角度来看，服务器不过就是高性能的计算机。但从网络应用的角度来看，服务器的地位是非常重要的，我们必须保证服务器与其他设备之间的连接具有非常高的可靠性。因此，服务器上经常需要用到链路聚合技术。

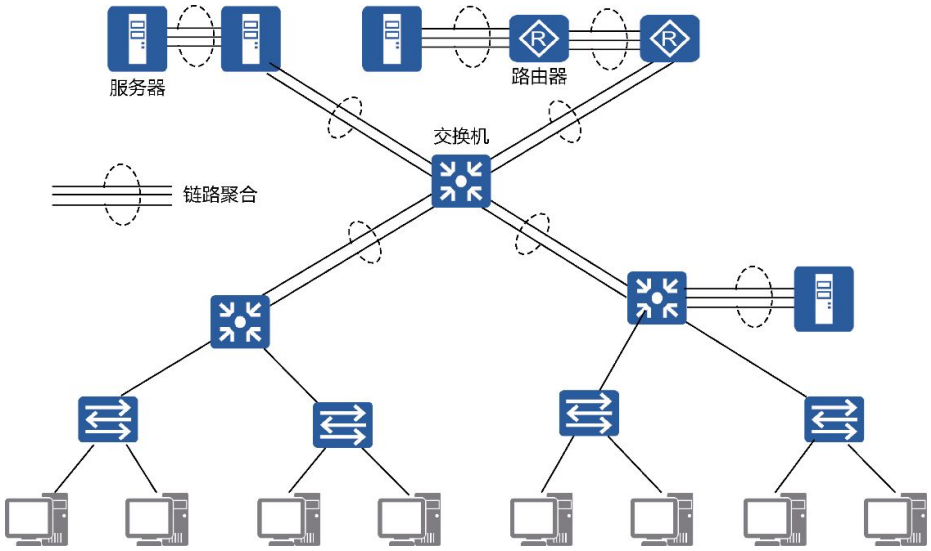


图7-30　链路聚合技术的适用场景

7.7.3　链路聚合的模式

建立链路聚合（后文称为Eth-Trunk）也像设置端口速率一样有手动配置和通过双方动态协商两种方式。在华为的Eth-Trunk语境中，前者称为手动模式（Manual Mode），而后者则根据协商协议被命名为了LACP模式（LACP Mode）。我们先从非常简单的手动配置方法说起。

1. 手动模式

采用Eth-Trunk的手动模式就像配置静态路由，或者在本地设置端口速率一样，都是一种把功能设置本地化、静态化的操作方式。说得具体一些，就是管理员在一台设备上创建出Eth-Trunk，然后根据自己的需求将多条连接到同一台交换机上的端口都添加到这个Eth-Trunk中，然后再在对端交换机上执行对应的操作。既然操作逻辑是把功能设置本地化，因此对于采用手动模式配置的Eth-Trunk，设备之间不会就建立Eth-Trunk而交互信息，它们只会按照管理员的操作执行链路捆绑，然后采用负载分担的方式通过捆绑的链路发送数据。

手动模式建立的Eth-Trunk就像静态添加到路由表中的路由条目那样，它比动态学习到的路由更加稳定，但缺乏灵活性。如果在手动模式配置的Eth-Trunk中有一条链路出现了故障，那么双方设备可以检测到这一点，并且不再使用那条故障链路，而继续使用仍然正常的链路来发送数据。尽管因为链路故障导致一部分带宽无法使用，但通信的效果仍然可以得到保障，如图7-31所示。

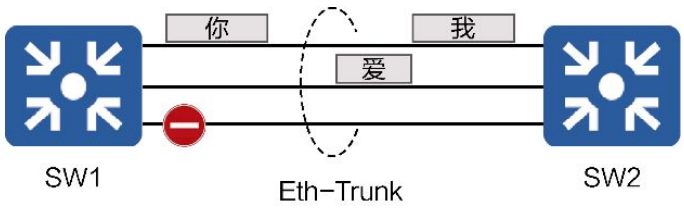


图7-31　手动模式Eth-Trunk使用故障链路外的其他链路执行负载分担

如图7-32所示，管理员误以为交换机SW1的接口GE0/0/0、GE0/0/1、GE0/0/2都和交换机SW2连接，因此将这三个接口划分到Eth-Trunk1的逻辑端口中了，SW1将毫不知情地使用GE0/0/2这个端口进行负载均衡，很显然“你”这个帧不能发送到交换机SW2。如果采用LACP模式，那么SW1和SW2之间使用LACP进行自动协商，从而可以容易地发现问题所在，SW1自动将GE0/0/2从Eth- Trunk中删除。

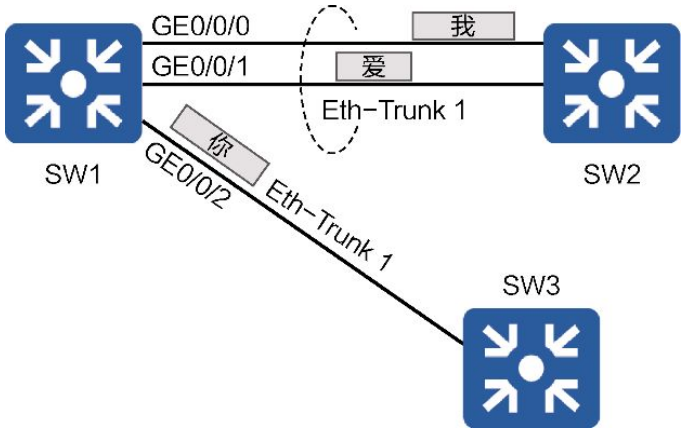


图7-32 手动模式Eth-Trunk配置错误无法正常通信

2. LACP模式

LACP为链路聚合控制协议（Link Aggregation Control Protocol），这个协议旨在为已建立链路聚合的设备之间提供协商和维护这条Eth-Trunk的标准。LACP模式Eth-Trunk的配置也不复杂，管理员只需要先在两边的设备上创建Eth-Trunk逻辑端口，然后将这个端口配置为LACP模式，最后再把需要捆绑的物理端口添加到这个Eth-Trunk中即可。

7.7.4 链路聚合配置示例

如图7-33所示，将交换机SW1的GEO/ 0/1、GEO/0/2、GEO/0/3和交换机SW2的GEO/0/1、GEO/0/2、GEO/0/3接口相连的三条链路配置成一条聚合链路。

在SW1上创建编号为1的Eth-Trunk端口，端口编号要和SW2的一致。配置Eth-Trunk 1端口的工作模式为手工负载分担模式，将端口GEO/0/1～GEO/0/3加入Eth-Trunk端口，将Eth-Trunk 1配置成干道链路，以允许所有VLAN通过。

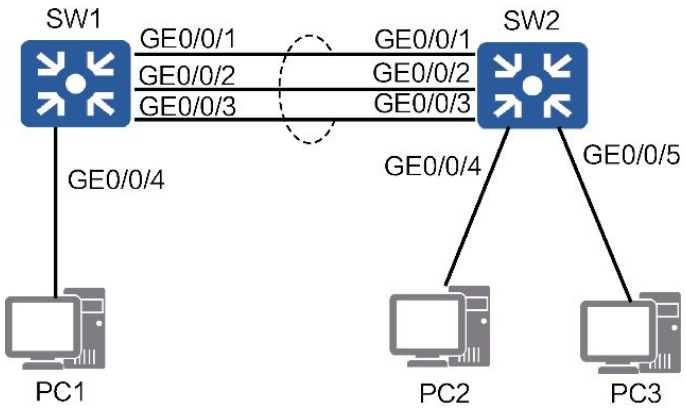


图7-33 Eth-Trunk配置示例

```
[SW1]interface Eth-Trunk 1
[SW1-Eth-Trunk1]mode ?
  lacp-static  Static working mode
  manual           Manual working mode
[SW1-Eth-Trunk1]mode manual load-balance
[SW1-Eth-Trunk1]trunkport GigabitEthernet 0/0/1 to 0/0/3
[SW1-Eth-Trunk1]port link-type trunk
[SW1-Eth-Trunk1]port trunk allow-pass vlan all
[SW1-Eth-Trunk1]quit
```

在SW2上创建编号为1的Eth-Trunk端口，端口编号要和SW1的一致。配置Eth-Trunk 1端口的工作模式为手工负载分担模式，将端口GE0/0/1～GE0/0/3加入Eth-Trunk端口，将Eth-Trunk 1配置成干道链路，以允许所有VLAN通过。

```
[SW2]interface Eth-Trunk 1
[SW2-Eth-Trunk1]mode manual load-balance
[SW2-Eth-Trunk1]trunkport GigabitEthernet 0/0/1 to 0/0/3
[SW2-Eth-Trunk1]port link-type trunk
[SW2-Eth-Trunk1]port trunk allow-pass vlan all
[SW2-Eth-Trunk1]quit
```

查看Eth-Trunk1端口的配置信息。

```
[SW1]display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL              Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
-
PortName                       Status      Weight
GigabitEthernet0/0/1        Up          1
GigabitEthernet0/0/2        Up          1
GigabitEthernet0/0/3        Up          1
```

在上面的回显信息中，“WorkingMode：NORMAL”表示Eth-Trunk1端口的工作模式为NORMAL，即手工负载分担模式（如果显示LACP，则表示工作模式为LACP模式）。“LeastActive-linknumber：1”表示处于Up状态的成员链路的下限阈值为1。“Operate status：up”表示Eth-Trunk 1端口的状态为Up。“Operate status: Up”表示Eth-Trunk1端口的状态为Up。“Number Of Up Port In Trunk:3”表明Eth-Trunk1有3个端口，PortName是端口名称。

7.8　习题

1．在下面关于VLAN的描述中，不正确的是（　　）。

A．VLAN把交换机划分成多个逻辑上独立的交换机

B．主干（Trunk）链路可以提供多个VLAN之间通信的公共通道

C．由于包含多个交换机，VLAN扩大了冲突域

D．一个VLAN可以跨越交换机

2．如图7-34所示，主机A跟主机C通信时，SWA与SWB间的Trunk链路传递的是不带VLAN标记的数据帧，但是当主机B跟主机D通信时，SWA与SWB之间的Trunk链路传递的是带VLAN标记20的数据帧。

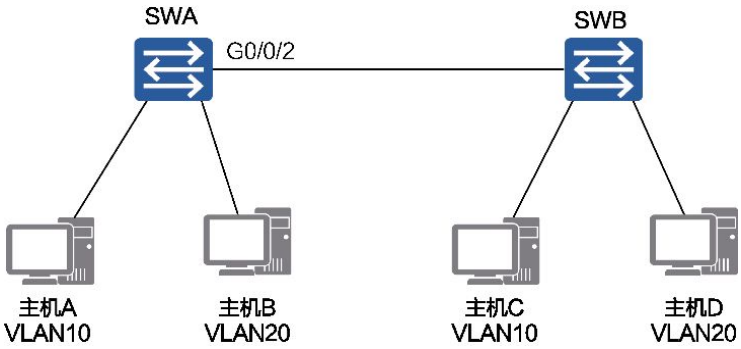


图7-34　通信示意图（一）

根据以上信息，下列描述中正确的是（　　）。

A．SWA上的G0/0/2端口不允许VLAN 10通过

B．SWA上的G0/0/2端口的PVID是10

C．SWA上的G0/0/2端口的PVID是20

D．SWA上的GO/O/2端口的PVID是1

3．以下关于生成树协议中的Forwarding状态的描述中，错误的是（　　）。

A．Forwarding状态的端口可以接收BPDU报文

B．Forwarding状态的端口不学习报文的源MAC地址

C．Forwarding状态的端口可以转发数据报文

D．Forwarding状态的端口可以发送BPDU报文

4．以下信息是运行STP的某交换机上所显示的端口状态信息。根据这些信息，以下描述中正确的是（　　）。

```
<S3>display stp brief
MSTID  Port                        Role    STP State           Protection
0    GigabitEthernet0/0/1          ALTE    DISCARDING          NONE
0    GigabitEthernet0/0/2          ROOT    FORWARDING          NONE
0    GigabitEthernet0/0/3          DESI    FORWARDING          NONE
```

A．此网络中有可能只包含这一台交换机

B．此交换机是网络中的根交换机

C．此交换机是网络中的非根交换机

D．此交换机肯定连接了3台其他的交换机

5．如图7-35所示，交换机与主机连接的端口均为Access端口，SWA的GO/O/1的PVID为2，SWB的GO/O/1的PVID为2，SWB的GO/O/3的PVID为3。SWA的GO/O/2为Trunk端口，PVID为2，且允许所有VLAN通过。SWB的GO/O/2为Trunk端口，PVID为3，且允许所有VLAN通过。

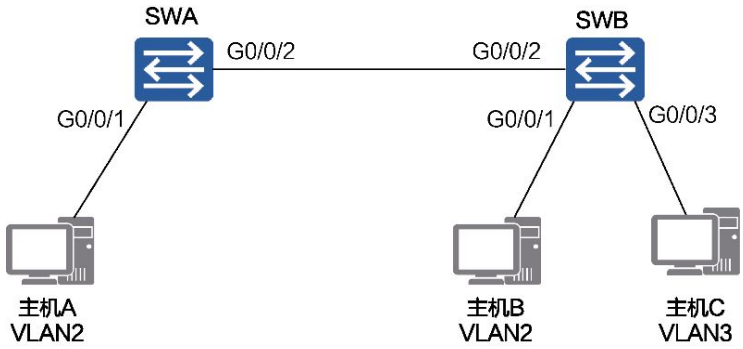


图7-35　通信示意图（二）

如果主机A、B和C的IP地址在一个网段，那么下列描述中正确的是（　　）。

A．主机A只可以与主机B通信

B．主机A只可以与主机C通信

C．主机A既可以与主机B通信，也可以与主机C通信

D．主机A既不能与主机B通信，也不能与主机C通信

6．使用单臂路由器实现VLAN间通信时，通常的做法是采用子端口，而不是直接采用物理端口，这是因为（　　）。

A．物理端口不能封装802.1Q

B．子端口转发速度更快

C．用子端口能节约物理端口

D．子端口可以配置Access端口或Trunk端口

7．使用命令“vlan batch 10 20”“vlan batch 10 to 20”分别能创建的VLAN数量是（　　）。

A．2和2

B．11和11

C．11和2

D．2和11

8．如图7-36所示，在SWA与SWB上创建VLAN 2，将连接主机的端口配置为Access端口，且属于VLAN 2。SWA的G 0/0/1与SWB的G 0/0/2都是Trunk端口，且允许所有VLAN通过。如果要使主机间能够正常通信，则网络管理员需要（　　）。

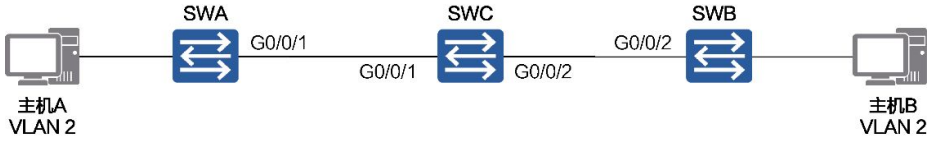


图7-36　通信示意图（三）

A．在SWC上创建VLAN 2即可

B．配置SWC上的G0/0/1为Trunk端口且允许VLAN 2通过即可

C．配置SWC上的G0/0/1和G0/0/2为Trunk端口且允许VLAN 2通过即可

D．在SWC上创建VLAN 2，配置G0/0/1和G0/0/2为Trunk端口，且允许VLAN 2通过

9．当二层交换网络中出现冗余路径时，用什么方法可以阻止环路产生、提高网络的可靠性？（　　）

A．生成树协议

B．水平分割

C．毒性逆转

D．触发更新

10．有用户反映在使用网络传输文件时，速度非常低，管理员在网络中使用Wireshark抓包工具发现了一些重复的帧，下面关于可能的原因或解决方案的描述中，正确的是（　　）。

A．交换机在MAC地址表中查不到数据帧的目的MAC地址时，会泛洪该数据帧

B．网络中的交换设备必须进行升级改造

C．网络的二层存在环路

D．网络中没有配置VLAN

11．链路聚合有什么作用？（　　）（选择3个答案）

A．增加带宽

B．实现负载分担

C．提升网络可靠性

D．便于对数据进行分析

12．在交换机上，哪些VLAN可以使用undo命令来删除？（　　）（选择3个答案）

A．VLAN 1

B．VLAN 2

C．VLAN 1024

D．VLAN 4096

13．如何保证某台交换机成为整个网络的根交换机？（　　）

A．为该交换机配置一个低于其他交换机的IP地址

B．设置该交换机的根路径开销值为最低

C．为该交换机配置一个低于其他交换机的优先级

D．为该交换机配置一个低于其他交换机的MAC地址

14．如图7-37所示，两台主机通过单臂路由器实现VLAN间通信，当RTA的G0/0/1.2子端口收到主机B发送给主机A的数据帧时，RTA将执行下列哪项操作？（　　）

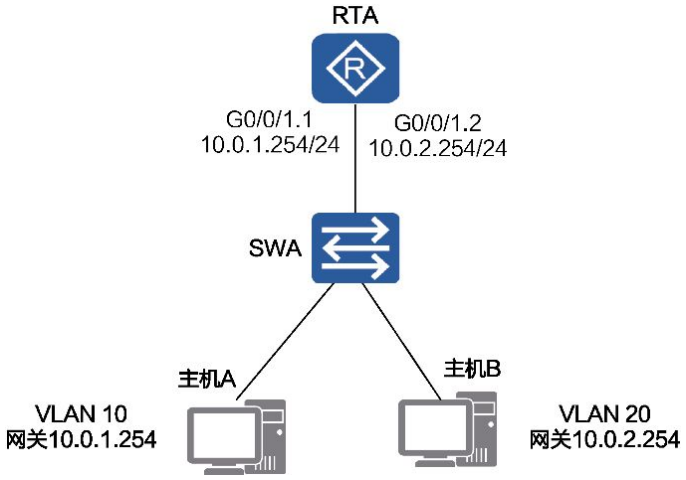


图7-37　通信示意图（四）

A．RTA将数据帧通过G0/0/1.1子端口直接转发出去

B．RTA删除VLAN 标记20后，由G0/0/1.1端口发送出去

C．RTA首先要删除VLAN标记20，然后添加VLAN标记10，再由G0/0/1.1端口发送出去

D．RTA将丢弃数据帧

15．下列关于VLAN配置的描述中，正确的是（　　）。

A．可以删除交换机上的VLAN 1

B．VLAN 1可以配置成Voice VLAN

C．所有Trunk端口默认允许VLAN 1的数据帧通过

D．用户能够配置使用VLAN 4095

16．交换机收到一个带有VLAN标记的数据帧，但是在MAC地址表中查不到该数据帧的目的MAC地址，下列描述中正确的是（　　）。

A．交换机会向所有端口广播该数据帧

B．交换机会向该数据帧所在VLAN的所有端口（除接收端口）广播此数据帧

C．交换机会向所有Access端口广播该数据帧

D．交换机会丢弃该数据帧

17．命令port trunk allow-pass vlan all 有什么作用？（　　）

A．在该端口上允许所有VLAN的数据帧通过

B．与该端口相连接的对端端口必须同时配置 port trunk permit vlan all

C．相连的对端设备可以动态确定允许哪些VLAN ID通过

D．如果为相连的远端设备配置了port default vlan 3命令，则两台设备之间的VLAN 3无法互通

18．在RSTP标准中，交换机直接与终端相连接而不是与其他网桥相连的端口被定义为（　　）。

A．快速端口

B．备份端口

C．根端口

D．边缘端口

19．下列关于Trunk端口与Access端口的描述中，正确的是（　　）。

A．Access端口只能发送untagged帧

B．Access端口只能发送tagged帧

C．Trunk端口只能发送untagged帧

D．Trunk端口只能发送tagged帧

20．STP计算的端口开销（port cost）和端口带宽有一定关系，即带宽越大，开销越（　　）。

A．小

B．大

C．一致

D．不一定

21．Access类型的端口在发送报文时，会（　　）。

A．发送带标记的报文

B．剥离报文的VLAN信息，然后发送出去

C．添加报文的VLAN 信息，然后发送出去

D．添加本端口的PVID信息，然后发送出去

22．如图7-38所示，在默认情况下，网络管理员希望使用Eth-Trunk手动聚合SWA与SWB之间的两条物理链路，下面描述中正确的是（　　）。

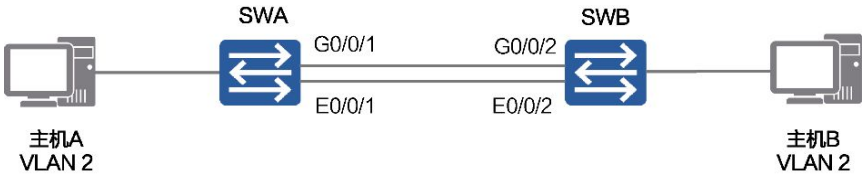


图7-38　通信示意图（五）

A．聚合后可以正常工作

B．可以聚合，聚合后只有G端口能收发数据

C．可以聚合，聚合后只有E端口能收发数据

D．不能聚合

23．某交换机端口属于VLAN 5，现在从VLAN 5中将该端口删除后，该端口属于哪个VLAN？（　　）

A．VLAN 0

B. VLAN 1

C. VLAN 1023

D. VLAN 1024

24. RSTP包含以下哪些端口状态？（　　）（多选）

A. Forwarding

B. Discarding

C. Listening

D. Learning

25. 设备链路聚合支持哪些模式？（　　）（多选）

A. 混合模式

B. 手动负载分担模式

C. 手动主备模式

D. LACP模式

第8章　网络安全

本章内容

- ACL简介
- 基本ACL
- 高级ACL
- AAA

路由器在不同网段转发数据包，为数据包选择路径。路由器也可以根据数据包的源IP地址、目标IP地址、协议、源端口、目标端口等信息过滤数据包。

数据包过滤通常控制哪些网段允许访问哪些网段，哪些网段禁止访问哪些网段。从源地址到目标地址画一个箭头，就能看到数据包经过哪些路由到达目的地，可以在数据包途经的任何路由器（当然这些路由器归你管理才行）上进行数据包过滤，数据包过滤可以在进路由器的端口或出路由器的端口上进行。确定了在哪个路由器的哪个端口，以及在哪个端口的哪个方向进行数据包过滤后，再创建访问控制列表（Access Control List，ACL），并在ACL中添加包过滤规则。

ACL分为基本ACL和高级ACL，基本ACL只能基于数据包的源地址、报文分片标记和时间段来定义规则。高级ACL可以根据数据包的源IP地址、目标IP地址、协议、目标端口、源端口、数据包的长度值来定义

规则。高级ACL与基本ACL相比，高级ACL在控制上更精准、更灵活、更复杂。

本章讲解基本ACL和高级ACL的用法，ACL规则的应用顺序，在ACL中添加规则、删除规则、插入规则，以及将ACL应用到路由器的端口。本章还会讲解AAA的工作方式和在路由器上的配置。

8.1 ACL简介

8.1.1 ACL的组成

如图8-1所示，一个ACL由若干条“拒绝1允许”（deny | permit）语句组成，每条语句都是该ACL的一条规则，每条语句中的deny或permit就是与这条规则相对应的处理动作。处理动作permit的含义是“允许”，处理动作deny的含义是“拒绝”。需要特别说明的是，ACL技术总是与其他技术结合在一起使用的，因此，所结合的技术不同，“允许”（permit）及“拒绝”（deny）的内涵及作用也会不同。例如，当ACL技术与流量过滤技术结合使用时，permit就是“允许通行”的意思，deny就是“拒绝通行”的意思。

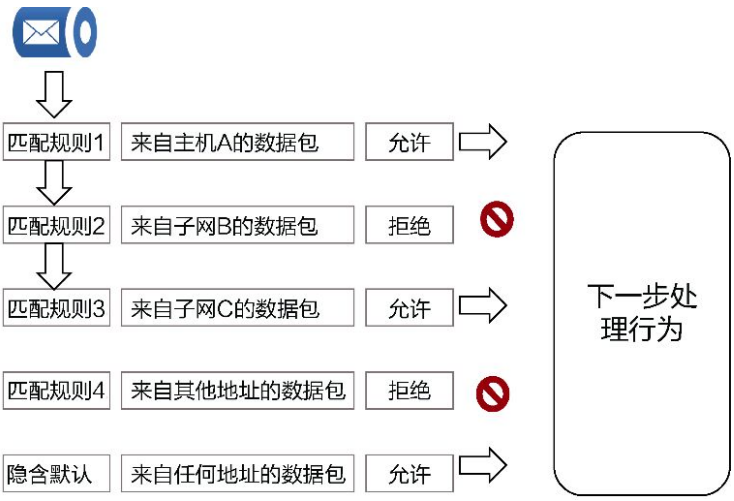


图8-1 ACL的组成

配置了ACL的设备在接收到一个报文之后，会将该报文与ACL中的规则逐条进行匹配。如果不能匹配上当前这条规则，则会继续尝试去

匹配下一条规则。一旦报文匹配上了某条规则，则设备会对该报文执行这条规则中定义的处理动作（permit或deny），并且不再继续尝试与后续规则进行匹配。如果报文不能匹配ACL的任何一条规则，则设备会对该报文执行permit这个处理动作。在华为路由器中的ACL隐含默认最后一条规则是任何地址都允许通过的。你也可以在ACL最后添加一条规则：拒绝来自任何地址的数据包。隐含默认的规则就没机会起作用了。

一个ACL中的每一条规则都有一个相应的编号，称为规则编号（rule-id）。默认情况下，报文总是按照规则编号从小到大的顺序与规则进行匹配。默认情况下，设备会在创建ACL的过程中自动为每一条规则分配一个编号。如果将规则编号的步长设定为10（注：规则编号的步长的默认值为5），则规则编号将按照10、20、30、40…这样的规律自动进行分配。如果将规则编号的步长设定为2，则规则编号将按照2、4、6、8…，这样的规律自动进行分配。步长的大小反映了相邻规则编号之间的间隔大小。间隔的存在，实际上是为了便于在两个相邻的规则之间插入新的规则。

8.1.2 ACL设计思路

使用ACL控制网络流量时，先考虑使用基本ACL还是使用高级ACL。如果只基于数据包源IP地址进行控制，就使用基本ACL。如果需要基于数据包的源IP地址、目标IP地址、协议、目标端口进行控制，那就需要高级ACL。然后再考虑在哪个路由器上的哪个接口的哪个方向进行控

制。确定了这些才能确定ACL规则中的哪些IP地址是源地址，哪些IP指定是目标地址。

在创建ACL规则前，还要确定ACL中规则的顺序，如果每条规则中的地址条件不叠加，则规则编号顺序无关紧要；如果多条规则中用到的地址有叠加，就要把地址块小的规则放到前面，地址块大的规则放到后面。

在路由器的每个接口的出向和入向的每个方向只能绑定一个ACL，一个ACL可以绑定多个接口。

如图8-2所示，R2路由器是企业内网连接Internet的路由器，在R2路由器上创建ACL以控制内网对Internet的访问。

在本节中，我们只想控制内网到Internet的访问，这是基于源IP地址的控制，因此使用基本ACL就可以实现。内网计算机访问Internet要经过R1和R2两个路由器，这就要考虑要在哪个路由器上进行控制，以及绑定到哪个接口。若在R1路由器上创建ACL，就要绑定到R1路由器的GE0/0/1的出向，在出去的时候检查应用ACL。本例在R2路由器上创建ACL，绑定到R2路由器的GE0/0/0的入向。

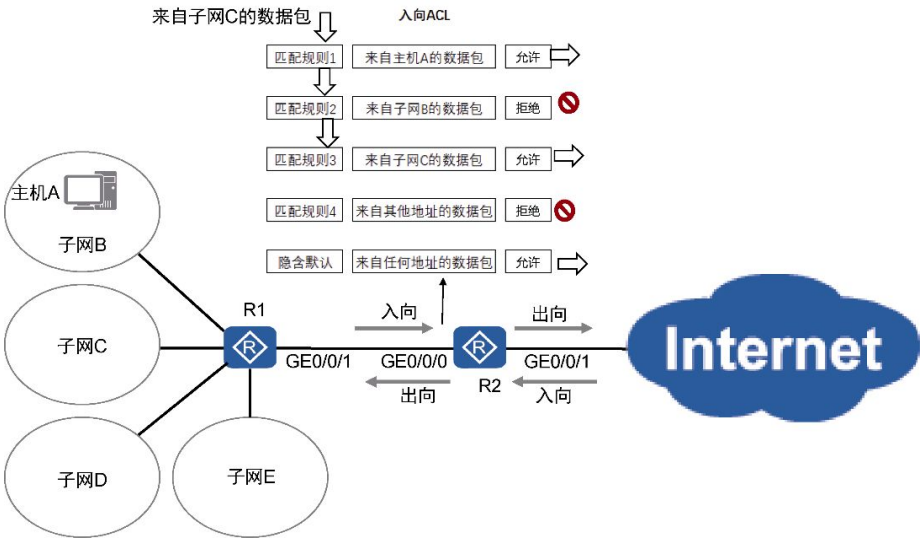


图8-2　ACL示例

可以看到图8-2中ACL中有4个匹配规则，在华为路由器中ACL隐含默认的最后一条规则是任何地址允许通过。本例中创建的匹配规则4为任何地址拒绝通过，则隐含默认规则就没机会用上了。因为ACL中的规则是按编号从小到大进行匹配，所以一旦匹配成功，就不再匹配下面的规则。

如果ACL中的每条规则包含的地址不叠加，则规则的应用顺序无关紧要，如果规则中地址有叠加，就要把地址块小的放到前面。比如图8-2中主机A的IP地址在子网B中，这就要求针对主机A的规则在针对子网C的规则前面，如果顺序颠倒，针对主机A的规则就没机会匹配上了。

创建好的ACL需要在接口进行绑定，并且要指明方向。方向是从路由器的方向来看的，从接口进入路由器就是入向，从接口出路由器就

是出向。本例中定义好的ACL绑定到R2路由器的GE0/0/0接口，那就是入向，绑定到R2路由器的GE0/0/1接口就是出向。

图8-2中来自子网C的数据包从R2路由器的GE0/0/0进入，将会依次比对规则1、规则2，最后匹配规则3，行为是允许进入。子网E在规则中没有明确指明，但会匹配规则4，拒绝进入，隐含默认那条规则没机会用到。

大家想一下，该ACL绑定到R2路由器的GE 0/0/1的出向是否可以？绑定到R2路由器的GE 0/0/1的入向是否可以？

8.2 使用基本ACL实现网络安全

ACL分为基本ACL和高级ACL。基本ACL只能基于数据包的源地址、报文分片标记和时间段来定义规则。根据数据包从源网络到目标网络的路径，在必经之地（某个路由器的端口）进行数据包过滤。在创建ACL之前，需要先确定在沿途的哪个路由器以及在哪个端口的哪个方向进行数据包过滤。

8.2.1 使用基本ACL实现内网安全

基本ACL只能基于IP报文的源IP地址、报文分片标记和时间段信息来定义规则。下面就以一家企业的网络为例，来讲述基本ACL的用法。

根据数据包从源网络到目标网络的路径，在必经之地（某个路由器的接口）进行数据包过滤。在创建ACL之前，需要先确定在沿途的哪个路由器的哪个接口的哪个方向进行包过滤，才能确定ACL规则的源地址。

如图8-3所示，某企业内网有三个网段，VLAN 10是财务部服务器，VLAN 20是工程部服务器，VLAN 30是财务部服务器。企业路由器AR1连接Internet，现需要在AR1上创建ACL以实现以下功能。

- 源IP地址为私有地址的流量不能从Internet进入企业网络。
- 财务部服务器只能由财务部中的计算机访问。

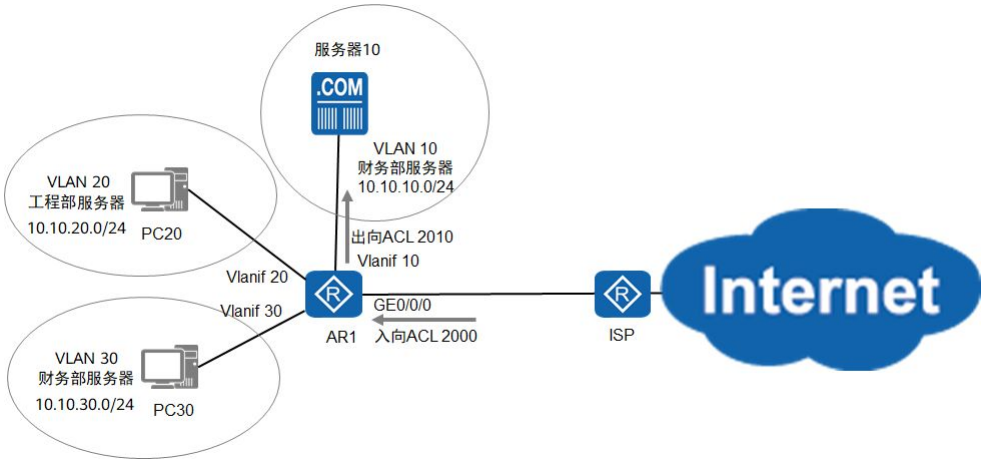


图8-3　企业网络

首先确定需要创建两个ACL，一个绑定到AR1路由器的GE0/0/0接口的入向，一个绑定到AR1的vlanif 10接口的出向。

在AR1上创建两个基本ACL：2000和2010。

```
[RA1]acl ?
  INTEGER<2000-2999>  Basic access-list(add to current using
rules) --基本ACL编号范围
  INTEGER<3000-3999>  Advanced access-list(add to current using
rules)--高级ACL编号范围
  INTEGER<4000-4999>  Specify a L2 acl group
  ipv6              ACL IPv6
  name               Specify a named ACL
  number             Specify a numbered ACL

[AR1]acl 2000
[AR1-acl-basic-2000]rule deny source 10.0.0.0 0.255.255.255
[AR1-acl-basic-2000]rule deny source 172.16.0.0 0.15.255.255
[AR1-acl-basic-2000]rule deny source 192.168.0.0 0.0.255.255
[AR1-acl-basic-2000]quit
[AR1]acl 2010
[AR1-acl-basic-2010]rule permit source 10.10.30.0 0.0.0.255
[AR1-acl-basic-2010]rule 20 deny source any                    --指
定规则编号
[AR1-acl-basic-2010]quit
```

在一个ACL中可以添加多条规则（rule），每条规则指定一个编号（Rule-ID），如果不指定，就由系统自动根据步长生成，默认步长为5。Rule-ID默认按照配置的先后顺序分配0、5、10、15，匹配顺序按照ACL的Rule-ID的值，从小到大进行匹配。不连续的Rule-ID编号方便我们以后插入规则，比如在Rule-ID为5和10的中间插入一条Rule-ID为7的规则。也可以根据Rule-ID删除规则。

输入display acl all查看全部ACL，输入display acl 2000可以查看编号是2000的ACL。

```
[AR1]display acl all
 Total quantity of nonempty ACL number is 2

Basic ACL 2000, 3 rules
Acl's step is 5
 rule 5 deny source 10.0.0.0 0.255.255.255
 rule 10 deny source 172.16.0.0 0.15.255.255
 rule 15 deny source 192.168.0.0 0.0.255.255

Basic ACL 2010, 2 rules
Acl's step is 5
 rule 5 permit source 10.10.30.0 0.0.0.255
 rule 20 deny
```

将创建好的ACL绑定到接口。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]traffic-filter inbound acl 2000
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface Vlanif 1
[AR1-Vlanif1]quit
[AR1]interface Vlanif 10
[AR1-Vlanif10]traffic-filter outbound acl 2010
[AR1-Vlanif10]quit
```

定义好ACL之后，还可以对其进行编辑，可以删除其中的规则，也可以在指定位置插入规则。

现在修改ACL 2000，删除其中的规则10，然后添加一条规则，以允许10.30.30.0/24网段通过。大家想想这条规则应该放到什么位置。

```
[RA1]acl 2000
[RA1-acl-basic-2000]undo rule 10  --删除rule 10
[RA1-acl-basic-2000]rule 2 permit source 10.30.30.0 0.0.0.255 --插入rule 2，编号要小于 5
[RA1-acl-basic-2000]rule 15 permit source 192.168.0.0 0.0.255.255 --修改rule 15，将其改成permit
[AR1-acl-basic-2000]display this
[V200R003C00]
#
acl number 2000
 rule 2 permit source 10.30.30.0 0.0.0.255
 rule 5 deny source 10.0.0.0 0.255.255.255
 rule 15 permit source 192.168.0.0 0.0.255.255
#
return
```

删除ACL，这并不自动删除接口的绑定，还需要在接口删除绑定的ACL。

```
[RA1]undo acl 2000
[RA1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]display this
[V200R003C00]
#
interface GigabitEthernet0/0/0
 ip address 20.1.1.1 255.255.255.0
 traffic-filter inbound acl 2000             --acl 2000依然绑定在出口
#
return
[AR1-GigabitEthernet0/0/0]undo traffic-filter inbound           --解除绑定
```

8.2.2 使用基本ACL保护路由器安全

网络中的路由器如果配置了VTY端口，那么只要网络畅通，任何计算机都可以telnet到路由器进行配置。一旦telnet路由器的密码被泄露，路由器的配置就有可能被非法更改。可以创建标准ACL，只允许特定IP地址能够telnet到路由器进行配置。

路由器AR1只允许PC3对其进行telnet登录。在AR1路由器上创建基本ACL 2001，并将之绑定到user-interface vty进站方向。

```
[RA1]acl 2001
[RA1-acl-basic-2001]rule permit source 192.168.2.2 0      --不指定步长，默认是5
[RA1-acl-basic-2001]rule deny source any                   --拒绝所有
```

提示：拒绝所有的代码可以简写成[RA1-acl-basic-2001]rule deny。

查看定义好的ACL 2001配置。

```
<RA1>display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5                              --步长为5
 rule 5 permit source 192.168.2.2 0 (1 matches)
 rule 10 deny (3 matches)
```

设置telnet端口的身份验证模式和登录密码，为用户权限级别绑定基本ACL 2001。

```
[RA1]user-interface vty 0 4
[RA1-ui-vty0-4]authentication-mode password                --设置身份验证模式
```

```
Please configure the login password (maximum length 16):91xueit --
设置登录密码91xueit
[RA1-ui-vty0-4]user privilege level 3
[RA1-ui-vty0-4]acl 2001 inbound                                  --绑定ACL
2001进站方向
```

删除绑定，请执行以下命令。

```
[RA1-ui-vty0-4]undo acl inbound
```

8.3　使用高级ACL实现网络安全

如图8-4所示，在AR1路由器上创建高级ACL以实现以下功能。

- 允许工程部访问Internet。
- 允许财务部访问Internet，但只允许访问网站和收发电子邮件。
- 允许财务部使用ping命令测试到Internet网络是否畅通。
- 禁止财务部服务器访问Internet。

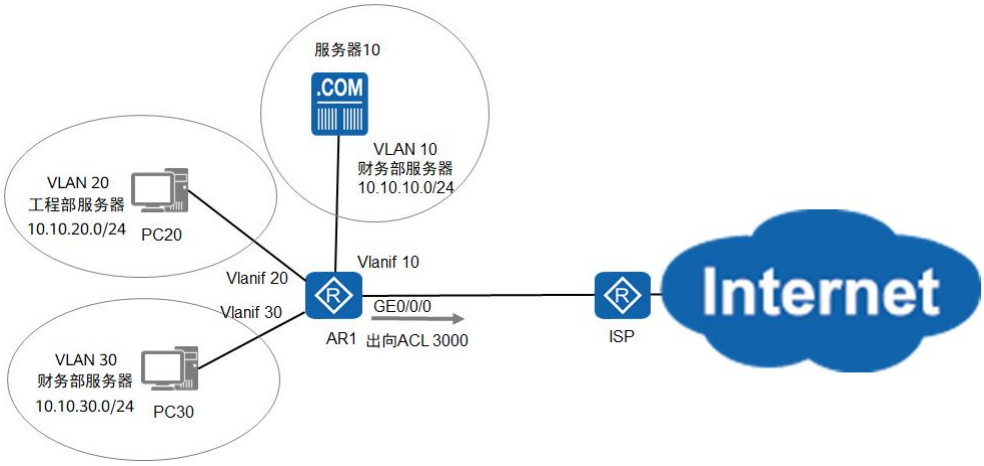


图8-4　高级ACL的应用

本案例实现的功能基于源地址和协议，此时就要使用高级ACL来实现。在AR1上创建一个高级ACL，将该ACL绑定到AR1的GE 0/0/0接口的出向。

允许财务部访问Internet网站，访问网站需要域名解析，域名解析使用的协议是DNS。DNS协议使用的是UDP的53端口，访问网站使用的协议是HTTP和HTTPS。HTTP使用的是TCP的80端口，HTTPS使用的是TCP的443端口。

为了避免以上实验创建的基本ACL对本实验的影响，先删除全部ACL，再在Vlanif 10和GE0/0/0上解除绑定的ACL。

```
[AR1]undo acl all     --删除以上实验创建的全部ACL
[AR1]interface Vlanif 10
[AR1-Vlanif10]undo traffic-filter outbound                --删除接口上的绑定
```

在AR1上创建高级ACL，规则中的协议是TCP或UDP时需要指定目标端口。

```
[AR1]acl 3000    --创建高级ACL
[AR1-acl-adv-3000]rule 5 permit ?    --查看可用的协议
  <1-255>  Protocol number
  gre      GRE tunneling(47)
  icmp     Internet Control Message Protocol(1)
  igmp     Internet Group Management Protocol(2)
  ip       Any IP protocol    --IP包含了TCP、UDP和ICMP
  ipinip  IP in IP tunneling(4)
  ospf     OSPF routing protocol(89)
  tcp      Transmission Control Protocol (6)
  udp      User Datagram Protocol (17)
[AR1-acl-adv-3000]rule 5 permit ip source 10.10.20.0 0.0.0.255
destination any
[AR1-acl-adv-3000]rule 10 permit udp source 10.10.30.0 0.0.0.255
destination any  ?
             --udp需要指定端口
  destination-port     Specify destination port
  dscp                 Specify dscp
  fragment             Check fragment packet
  none-first-fragment  Check the subsequence fragment packet
……

[AR1-acl-adv-3000]rule 10 permit udp source 10.10.30.0 0.0.0.255
destination any
 destination-port ? --指定大于、小于或等于哪个端口或端口范围
  eq        Equal to given port number
  gt        Greater than given port number
  lt        Less than given port number
  range     Between two port numbers
[AR1-acl-adv-3000]rule 10 permit udp source 10.10.30.0 0.0.0.255
destination any
 destination-port eq ? --可以指定端口号或应用层协议名称
```

```
  <0-65535>        Port number
  biff             Mail notify (512)
  bootpc           Bootstrap Protocol Client (68)
  bootps           Bootstrap Protocol Server (67)
  discard          Discard (9)
  dns              Domain Name Service (53)
  dnsix            DNSIX Security Attribute Token Map (90)
  echo             Echo (7)
  ……
[AR1-acl-adv-3000]rule 10 permit udp source 10.10.30.0 0.0.0.255
destination any
 destination-port eq dns
[AR1-acl-adv-3000]rule 15 permit tcp source 10.10.30.0 0.0.0.255
destination-port eq www
[AR1-acl-adv-3000]rule 20 permit tcp source 10.10.30.0 0.0.0.255
destination-port eq 443
[AR1-acl-adv-3000]rule 25 permit icmp source 10.10.30.0 0.0.0.255
[AR1-acl-adv-3000]rule 30 deny ip
[AR1-acl-adv-3000]quit
```

将ACL绑定到接口。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]traffic-filter outbound acl 3000
```

8.4 AAA

网络设备或操作系统通常有多个用户登录访问，不同的用户可以设置不同的访问权限，为了安全还需要跟踪并记录用户的访问行为。

用户登录系统或网络设备时需要输入账户密码来验证用户的身份，这个过程叫作身份认证（authentication）。不同的用户被授予了不同的权限，这个过程叫作授权（authorization）。为了安全，用户登录后对系统资源的访问或更改进行记录，这个过程叫作审计（accounting），这三项独立安全功能总称为AAA。审计功能不在本节讨论。

8.4.1 AAA工作方式

网络设备可以通过两种不同的方式对发起管理访问的用户执行认证、授权和审计，其中一种方式是在本地完成的。如图8-5所示，网络设备通过自己本地数据库中的用户名和密码信息来完成身份验证、权限指定和操作记录。

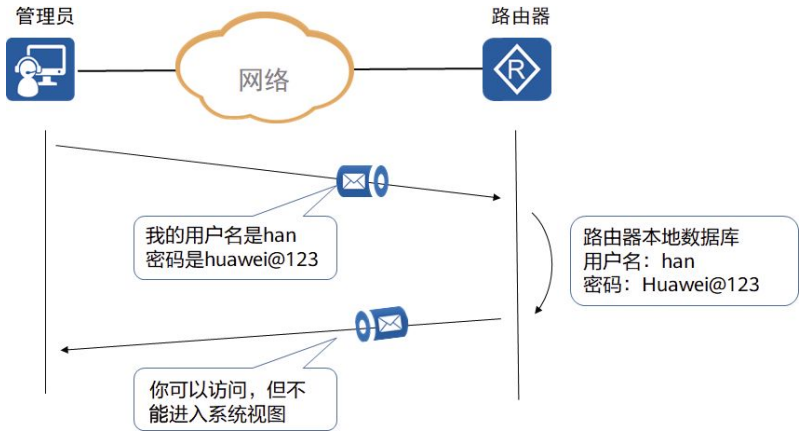


图8-5　本地AAA的工作方式示意图

另一种方式是通过外部的AAA服务器来完成。当用户向网络设备发起管理访问时，网络设备向位于指定地址的AAA服务器发送查询信息，让AAA服务器判断是否允许这位用户访问，以及这位用户拥有什么权限等，如图8-6所示。

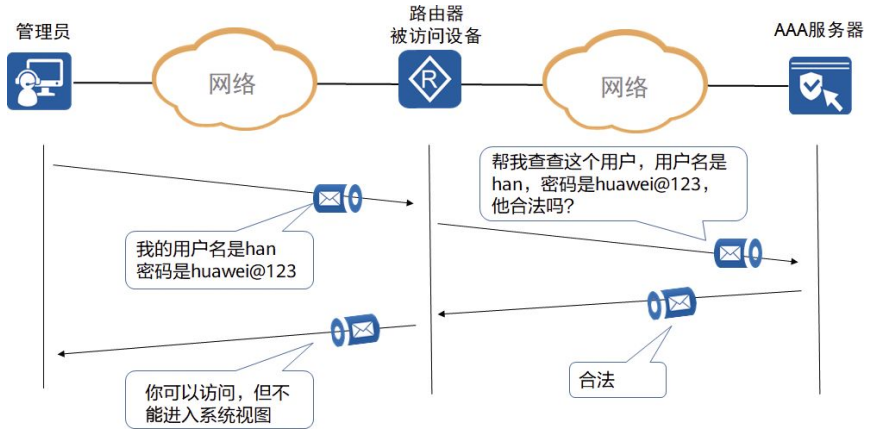


图8-6　通过AAA服务器执行AAA的工作方式示意图

与在设备本地执行AAA操作相比，通过AAA服务器来为网络集中提供AAA服务最直接的优势源于扩展性。因此，在中到大规模网络中，图8-5所示的这种依靠AAA服务器来集中提供AAA服务的做法更加常见。在

这种环境中，人们当然需要定义被管理设备与AAA服务器之间通信的标准。RADUIS协议就是被管理设备和AAA服务器通信的标准协议，即远程认证拨入用户服务（Remote Authentication Dial In User Service），AAA服务器是RADUIS服务器，路由器是RADUIS客户端。

通过AAA服务器执行AAA工作方式以及RADIUS协议在本书不做过多介绍。

8.4.2 AAA的配置

本节展示如何配置华为路由器AAAA本地认证。使用telnet远程登录华为路由器时，可以使用密码（password）认证，但使用密码认证没有办法针对不同的用户设置不同的权限。为了提高安全性，为不同的用户授予不同的访问权限，就需要设置telnet登录使用AAA进行本地认证。本示例使用的网络环境如图8-7所示。

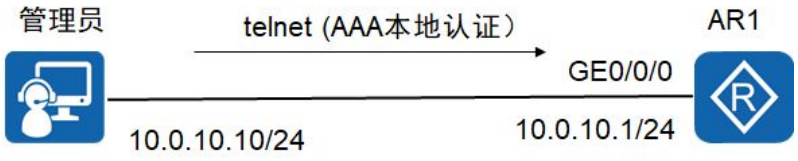


图8-7　使用AAA本地认证的方式进行登录验证

在这个环境中，我们要在路由器AR1上针对telnet启用AAA本地认证，对通过telnet向AR1发起管理访问的用户进行认证。用户只有输入了正确的用户名和密码，才能够成功登录AR1。

在华为网络设备上，默认情况下有一个名为default的认证方案（authentication-scheme），管理员不能删除这个认证方案，但能够对其进行修改。在认证方案default中，默认的认证模式为本地认证（local，也就是说，路由器会使用本地数据库对用户的登录行为进行认证。在这个示例中，我们就直接使用认证方案default，并且保留默认认证模式Iocal不做修改。

查看AR1上默认的AAA配置信息：

```
[AR1]aaa
[AR1-aaa]display this
[V200R003C00]
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
return
[AR1-aaa]
```

在本例中管理员先使用系统视图命令aaa进入了AAA视图，然后在AAA视图中使用了命令display this，这条命令能够查看当前视图中的配置命令。在命令display this的输出内容中，重点介绍authentication-scheme default和domain default_admin。

- authentication-scheme default：这是默认的认证方案default。如果在AAA视图中输入命令authentication-scheme default，就可以进入default认证方案的视图，并修改default中的参数。在default认证方案视图中，管理员可以使用

authentication-mode local命令设置本地认证模式。由于这是默认的认证模式，所以即使管理员输入了这条命令，在配置中也看不到该设置。

```
[AR1-aaa]authentication-scheme default
[AR1-aaa-authen-default]authentication-mode ?
  hwtacacs   HWTACACS
  local      Local
  none       None
  radius     RADIUS
[AR1-aaa-authen-default]authentication-mode local
```

- domain default_admin：这是默认的管理员域default_admin，也就是通过HTTP、SSH、Telnet、Terminal或FTP方式进行设备登录的用户所属的域。如果在AAA视图中输入命令domain default_admin，就可以进入default_admin域视图，并修改这个域中的参数。

```
[AR1-aaa]domain default_admin
[AR1-aaa-domain-default_admin]?
aaa-domain-default_admin view commands:
  accounting-scheme      Configure accounting scheme
  arp-ping               ARP-ping
  authentication-scheme  Configure authentication scheme
  authorization-scheme   Configure authorization scheme
  backup                 Backup  information
 ……
```

对于通过Telnet的方式登录设备的用户来说，用户属于default_admin域，这个域使用默认的default认证方案，default认证方案中又设置了默认的本地认证模式。在这个层层嵌套的配置中，如果想要通过AAA本地认证对Telnet进行保护，那么管理员无须进行任何修改。因此接下来需要做的是创建用来进行Telnet登录的本地用户。

以下命令在AR1路由器上创建了两个用户user1和user2。在创建user1时，管理员指定了用户名（user1）和密码（huawei111），并且把user1的接入服务类型设置为Telnet。在创建user2时，管理员除了指定用户名（user2）和密码（huawei222），并且把user2的接入服务类型也设置为Telnet外，还指定了user2的级别15，也就是最高级别。管理员没有为user1指定级别，因此user1的级别为默认级别0，也就是最低级别。

```
[AR1]aaa
[AR1-aaa]local-user user1 password cipher huawei111
Info: Add a new user.
[AR1-aaa]local-user user1 service-type telnet
[AR1-aaa]local-user user2 privilege level 15 password cipher
huawei222
Info: Add a new user.
[AR1-aaa]local-user user2 service-type telnet
```

最后，管理员还需要配置VTY线路，把它的认证模式设置为AAA。

```
[AR1]user-interface vty 0 4
[AR1-ui-vty0-4]authentication-mode aaa
[AR1-ui-vty0-4]quit
```

使用user1账户Telnet AR1路由器。登录成功后，输入问号查询当前能够使用的命令，发现命令非常有限，因为user1的级别是0。图8-8展示了user1登录后可用的命令。

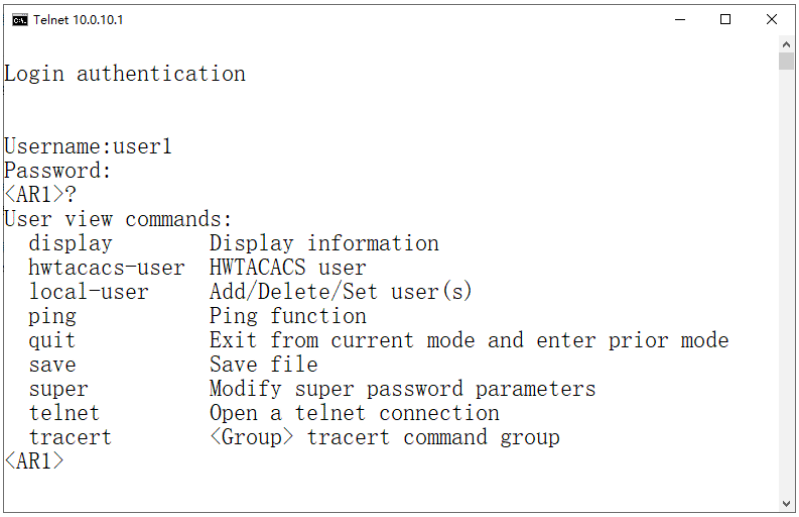


图8-8　使用user1进行登录测试

使用user2登录，结果如图8-9所示。输入问号查询当前能够输入的配置命令，发现user2能够使用的命令非常多，这是因为user2的级别是15，也就是最高级别，说明user2能够使用全部命令。

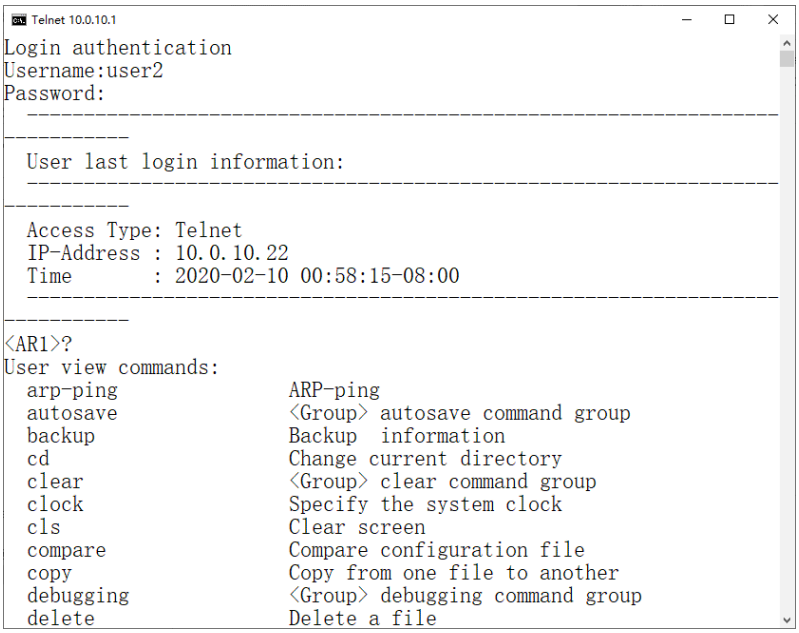


图8-9　使用user2进行登录测试

通过命令display local-user，可以查看设备本地配置的用户信息。

```
   [AR1]display local-user
------------------------------------------------------------------------------
   User-name                      State   AuthMask  AdminLevel
------------------------------------------------------------------------------
  admin                            A      H         -
  user1                            A      T         -
  user2                            A      T         15
------------------------------------------------------------------------------
  Total 3 user(s)
[AR1]
```

在以上输出中，State是A（Active）标明该用户处于活动状态，B（Block）标明该用户处于禁用状态。AuthMask表示本地用户的接入类型，admin的接入类型为H（HTTP），user1和user2的接入类型为T（telnet），接入类型还有S（SSH）、F（FTP）等。AdminLevel表示本地用户的管理员用户级别，从这里也可以看出user2的级别为15。

通过命令display local-user username *username*，可以查看某个用户的信息，下面查看user2的信息。

```
[AR1]display local-user username user2
  The contents of local user(s):
  Password           : ****************
  State              : active
  Service-type-mask  : T
  Privilege level    : 15
  Ftp-directory      : -
  Access-limit       : -
  Accessed-num       : 0
  Idle-timeout       : -
  User-group         : -
```

8.5 习题

1．关于访问控制列表编号与类型的对应关系，下列描述中正确的是（　　）。

A．基本的访问控制列表编号范围是1000～2999

B．高级的访问控制列表编号范围是3000～4000

C．二层的访问控制列表编号范围是4000～4999

D．基于端口的访问控制列表编号范围是1000～2000

2．在路由器RTA上完成如下所示的ACL配置，则下面描述中正确的是（　　）。

```
[RTA]acl 2001
[RTA-acl-basic-2001]rule 20 permit source 20.1.1.0 0.0.0.255
[RTA-acl-basic-2001]rule 10 deny source 20.1.1.0 0.0.0.255
```

A．VRP系统将会自动按配置的先后，顺序调整第一条规则的顺序编号为5

B．VRP系统不会调整顺序编号，但是会先匹配第一条配置的规则permit source 20.1.1.0 0.0.0.255

C．配置错误，规则的顺序编号必须从小到大配置

D．VRP系统将会按照顺序编号，先匹配第二条规则deny source 20.1.1.0 0.0.0.255

3．ACL中的每条规则都有相应的规则编号以表示匹配顺序。在如下所示的配置中，关于两条规则的编号的描述中，正确的是（　　）。（选择两个答案）

```
[RTA]acl 2002
[RTA-acl-basic-2002]rule permit source 20.1.1.10
[RTA-acl-base-2002]rule permit source 30.1.1.10
```

A．第一条规则的顺序编号是1

B．第一条规则的顺序编号是5

C．第二条规则的顺序编号是2

D．第二条规则的顺序编号是10

4．如图8-10所示，网络管理员希望主机A 不能访问WWW服务器，但是不限制其访问其他服务器，则下列RTA的ACL中能够满足需求的是（　　）。

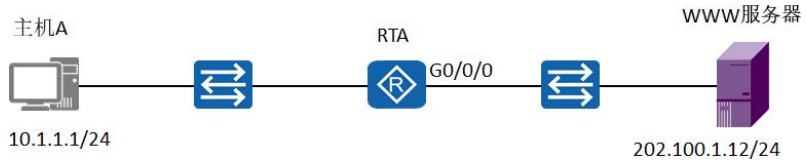


图8-10　通信示意图（一）

A. rule deny tcp source 10.1.1.10 destination 202.100.1.12 0.0.0.0 destination-port eq 21

B. rule deny tcp source 10.1.1.10 destination 202.100.1.12 0.0.0.0 destination-port eq 80

C. rule deny udp source 10.1.1.10 destination 202.100.1.12 0.0.0.0 destination-port eq 21

D. rule deny udp source 10.1.1.10 destination 202.100.1.12 0.0.0.0 destination-port eq 80

5. 一台AR2220路由器上使用如下ACL配置来过滤数据包，则下列描述中正确的是（　　）。

```
[RTA]acl 2001
[RTA-acl-basic-2001]rule permit source 10.0.1.0 0.0.0.255
[RTA-acl-basic-2001]rule deny source 10.0.1.0 0.0.0.255
```

A. 10.0.1.0/24网段的数据包将被拒绝

B. 10.0.1.0/24网段的数据包将被允许

C. 该ACL配置有误

D. 以上选项都不正确

6. 如图8-11所示，网络管理员在路由器RTA上使用ACL 2000过滤数据包，则下列描述中正确的是（　　）。（选择两个答案）

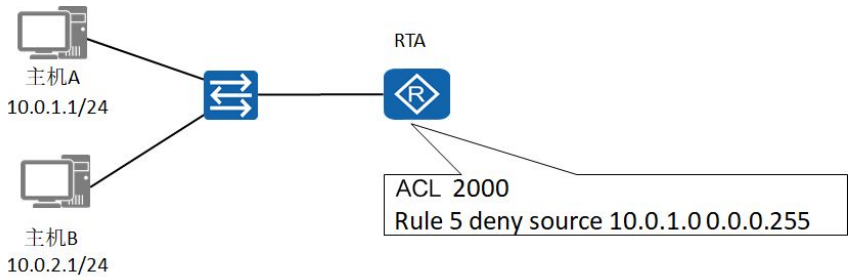


图8-11　通信示意图（二）

A．RTA转发来自主机A的数据包

B．RTA丢弃来自主机A的数据包

C．RTA转发来自主机B的数据包

D．RTA丢弃来自主机B的数据包

7．在路由器PTA上使用如下所示的ACL匹配路由条目，则下列哪些条目将会被匹配上？（选择两个答案）

```
[RTA]acl 2002
[RTA-acl-basic-2002]rule deny source 172.16.1.1 0.0.0.0
[RTA-acl-basic-2002]rule deny source 172.16.0.0 0.0.255.255
```

A．172.16.1.1/32

B．172.16.1.0/24

C．192.17.0.0/24

D．172.18.0.0/16

8．下列哪项参数不能用于高级访问控制列表？（　　）

A．物理端口

B．目的端口号

C．协议号

D．时间范围

9．某个ACL规则如下，则下列哪些IP地址可以被permit规则匹配？（　　）（多选）

```
rule 5 permit ip source 10.1.1.0 255.0.254.255
```

A．7.1.2.1

B．6.1.3.1

C．8.2.2.1

D．9.1.1.1

10．用Telnet方式登录路由器时，可以选择哪几种认证方式？（　　）（多选）

A．AAA本地认证

B．不认证

C．password认证

D．MD5密文认证

11．如图8-12所示，在RTA路由器上创建ACL，禁止10.0.1.1/24、10.0.2.1/24和10.0.3.1/ 24网段之间相互访问，并允许这3个网段访问Internet。考虑使用基本ACL还是高级ACL，考虑ACL绑定的位置和方向。创建ACL，并绑定到适当端口。

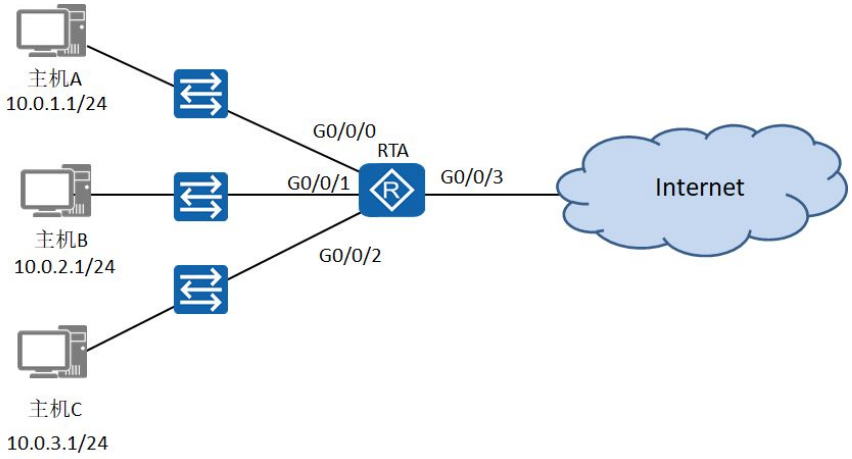


图8-12　通信示意图（三）

第9章　网络地址转换和端口映射

本章内容

- 介绍公网地址和私网地址
- NAT的类型
- 静态NAT的实现
- NAPT的实现
- Easy IP的实现
- 配置端口映射
- 灵活运用NAPT

本章介绍公网IP地址和私网IP地址，企业内网通常使用私网IP地址，Internet使用的是公网IP地址。使用私网地址的计算机访问Internet（公网）时需要用到网络地址转换（Network Address Translation，NAT）技术。

在连接企业内网（私网地址）和Internet的路由器上配置网络地址转换（NAT）。一个私网地址需要占用一个公网地址做转换。NAT分为静态NAT和动态NAT。

如果内网计算机数量（私网地址数量）比可用的公网地址多，就需要做网络地址端口转换（Network Address and Port Translation，NAPT）。NAPT技术允许企业内网的计算机使用公网IP地址进行网络地址端口转换。

如果企业的服务器部署在内网，使用私网地址，若想让Internet上的计算机访问内网服务器，就需要在连接Internet的路由器上配置端口映射。

9.1　公网地址和私网地址

公网指的是Internet，公网IP地址指的是Internet上全球统一规划的IP地址，网段地址块不能重叠。Internet上的路由器能够转发目标地址为公网地址的数据包。

在IP地址空间中，A、B、C 3类地址中各保留了一部分地址作为私网地址。私网地址不能在公网上出现，只能用在内网中，Internet中的路由器没有到私网地址的路由。

保留的A、B、C类私网地址的范围分别如下。

A类地址：10.0.0.0～10.255.255.255。

B类地址：172.16.0.0～172.31.255.255。

C类地址：192.168.0.0～192.168.255.255。

企业或学校的内部网络，可以根据计算机数量、网络规模大小来选用适当的私网地址段。小型企业或家庭网络可以选择保留的C类私网地址，大中型企业网络可以选择保留的B类地址或A类地址。如图9-1所示，A学校选用10.0.0.0/28作为内网地址，B学校也选择10.0.0.0/28作为内网地址，反正这两个学校的网络现在不需要相互通信，将来也不打算相互访问，因此使用相同的网段或地址重叠也没关系。如果以后A学校和B学校的网络需要相互通信，就不能使用重叠的地址段了，就要重新规划这两个学校的内网地址。

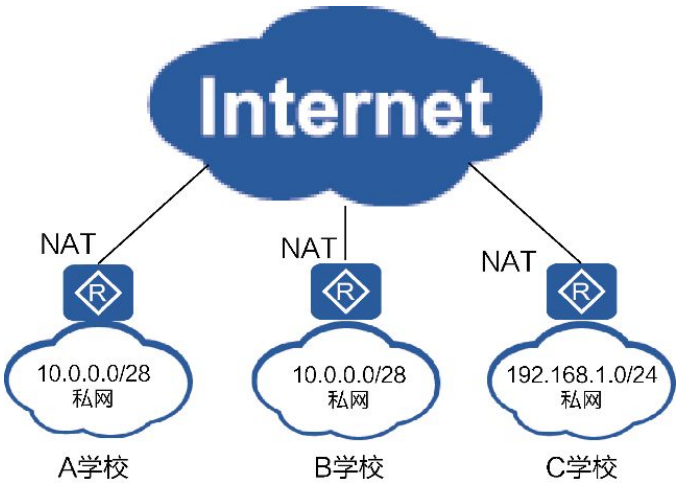


图9-1 私网地址

企业内网使用私网地址，可以减少对公网地址的占用。NAT一般应用在边界路由器中，比如公司连接Internet的路由器上。NAT的优缺点如表9-1所示。

表9-1 NAT的优缺点

优　　点	缺　　点

优　　点	缺　　点
● 通过使用NAPT技术，企业私网访问Internet时可以使用公网地址，节省公网IP地址 ● 更换ISP，内网地址不用更改，增强Internet连接的灵活性 ● 私网在Internet上不可直接访问，增强内网的安全性	● 在路由器上做NAT或NAPT，都需要修改数据包的网络层和传输层，并且会在路由器中保留、记录端口地址转换对应关系。这相比路由数据包会产生较大的交换延迟，同时会消耗路由器较多的资源 ● 使用私网地址访问Internet，源地址被替换成公网地址。如果某学校的学生在论坛上发布谣言，论坛只能记录发帖人的IP地址是该学校的公网地址，没办法跟踪到是内网的哪个地址，也就是无法进行端到端的IP跟踪 ● 公网不能访问私网计算机，如需访问，要做端口映射 ● 某些应用无法在NAT网络中运行，比如IPSec不允许中间数据包被修改

9.2 NAT的类型

下面介绍NAT的4种类型：静态NAT、动态NAT、地址池NAPT和Easy IP。

9.2.1 静态NAT

静态NAT在连接私网和公网的路由器上进行配置，一个私网地址对应一个公网地址，这种方式不节省公网IP地址。

如图9-2所示，在R1路由器上配置静态映射，内网192.168.1.2访问Internet时使用公网地址12.2.2.2替换源IP地址；内网192.168.1.3访问Internet时使用公网地址12.2.2.3替换源IP地址。图9-2展现了PC1、PC2访问Web服务器，数据包在内网时的源地址和目标地址，以及数据包发送到Internet后的源地址和目标地址，也展现了Web服务器发送给PC1和PC2的数据包在Internet的源地址和目标地址，以及进入内网后的源地址和目标地址。

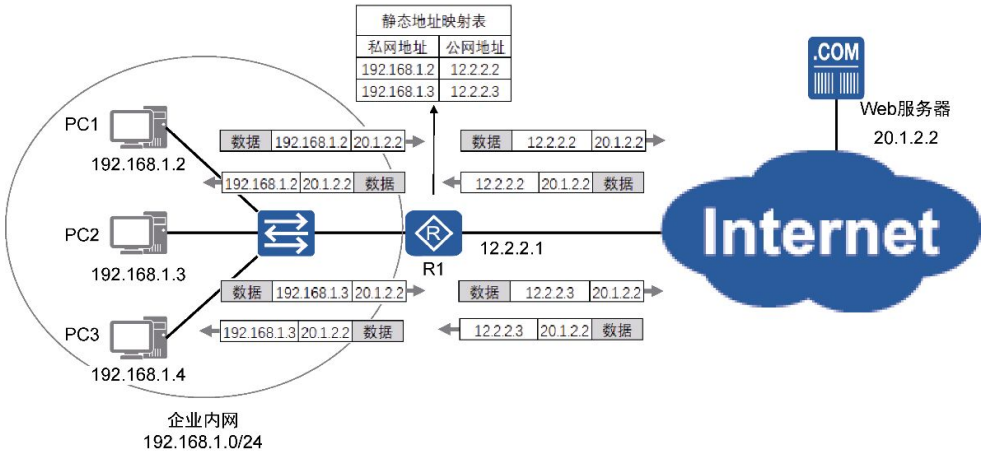


图9-2　静态NAT示意图

PC3不能访问Internet，因为R1路由器没有为IP地址192.168.1.4指定用来替换的公网地址。配置好了静态NAT，Internet上的计算机就能通过访问12.2.2.2来访问内网的PC1，通过访问12.2.2.3来访问内网的PC2。

静态NAT使得内网能够访问Internet，同样Internet上的计算机通过访问静态地址映射表中的某个公网地址来访问对应的内网计算机。

9.2.2　动态NAT

动态NAT在连接私网和公网的路由器上进行配置，在路由器上创建公网地址池（地址段），并使用ACL定义内网地址，并不指定用哪个公网地址替换哪个私网地址。内网计算机访问Internet时，路由器会从公网地址池中随机选择一个没被使用的公网地址做源地址替换。动态NAT只允许内网主动访问Internet，Internet上的计算机不能通过公网地址访问内网的计算机，这和静态NAT不一样。

如图9-3所示，内网有4台计算机，公网地址池有3个公网IP地址，这只允许内网的3台计算机访问Internet，到底谁能访问Internet，那就看谁先上网了。图9-3中PC4没有可用的公网地址，就不能访问Internet了。

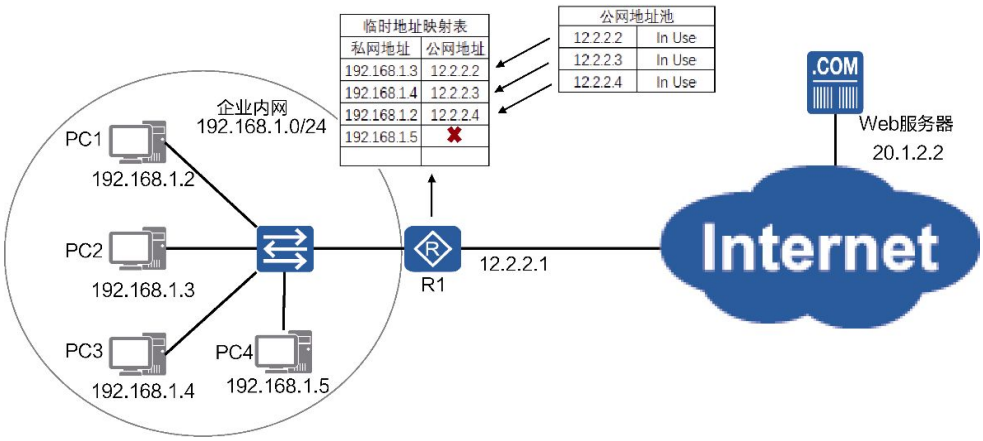


图9-3　动态NAT

9.2.3　网络地址端口转换（NAPT）

如果用于NAT的公网地址少于内网中上网计算机的数量，那么在内网计算机使用公网地址池中的IP地址访问Internet时，出去的数据包就要替换源IP地址和源端口。路由器中有一张表用于记录端口地址转换，如图9-4所示。

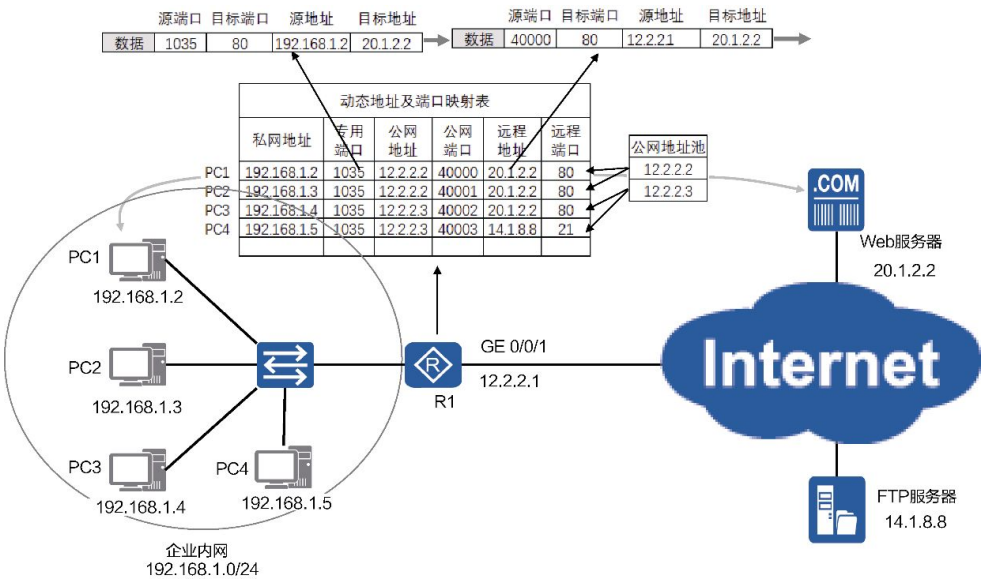


图9-4　网络地址端口转换示意图

源端口（图9-4中的公网端口）由路由器统一分配，不会重复。R1收到返回来的数据包，根据目标端口就能判定应该给内网中的哪台计算机。这就是网络地址端口转换（Network Address and Port Translation，NAPT），应用NAPT会节省公网地址。

NAPT只允许内网主动访问Internet，Internet中的计算机不能主动向内网发起通信，这使得内网更加安全。

9.2.4 Easy IP

Easy IP技术是NAPT的一种简化情况。Easy IP无须建立公有IP地址资源池，因为Easy IP只会用到一个公有地址，该地址就是路由器R1的GE 0/0/1接口的IP地址。Easy IP也会建立并维护一张动态地址及端口映射表，并且，Easy IP会将这张表中的公有IP地址与GE 0/0/1接口的IP地址绑定。R1的GE 0/0/1接口的IP地址如果发生了变化，那么，这张表中的公有IP地址也会自动跟着变化。GE 0/0/1接口的IP地址可以是手动配置的，也可以是动态分配的。

在其他方面，Easy IP是与NAPT完全一样的，这里不再赘述。

9.3　静态NAT的实现

在连接Internet的路由器上配置静态NAT。

如图9-5所示，企业内网的私网地址是192.168.0.0/24，AR1路由器连接Internet，有一条默认路由指向AR2的GE 0/0/0端口地址。AR2代表ISP的Internet上的路由器，该路由器没有到私网的路由。ISP给企业分配了3个公网地址12.2.2.1、12.2.2.2、12.2.2.3，其中12.2.2.1指定给AR1的GE 0/0/1端口。

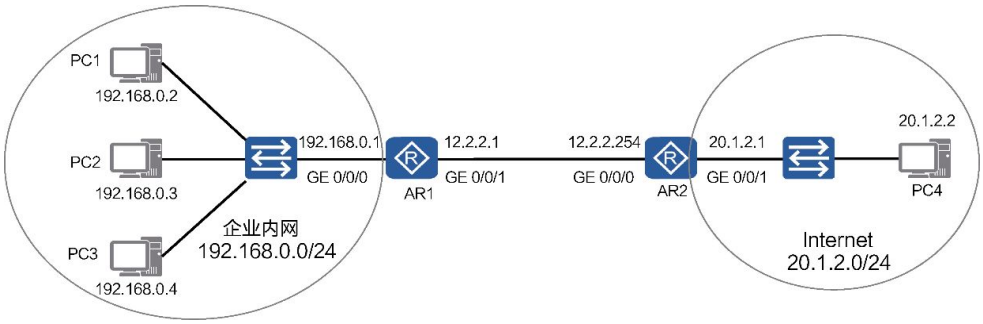


图9-5　配置静态NAT

现在要求在AR1路由器上配置静态NAT，PC1访问Internet的IP地址使用12.2.2.2替换、PC2访问Internet的IP地址使用12.2.2.3替换。12.2.2.1地址已经分配给AR1的GE 0/0/1端口使用了，静态映射不能再使用这个地址。

在配置静态NAT之前，内网计算机是不能访问Internet上的计算机的。思考一下为什么？是数据包不能到达目标地址，还是Internet上的计算机发出的响应数据包不能返回内网？

在AR1上配置静态NAT。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]nat static global 12.2.2.2 inside
192.168.0.2
[AR1-GigabitEthernet0/0/1]nat static global 12.2.2.3 inside
192.168.0.3
```

查看NAT静态映射。

```
<AR1>display nat static
 Static Nat Information:
 Interface  : GigabitEthernet0/0/1
   Global IP/Port     : 12.2.2.2/----
   Inside IP/Port    : 192.168.0.2/----
   Protocol : ----
   VPN instance-name  : ----
   Acl number     : ----
   Netmask  : 255.255.255.255
   Description : ----

   Global IP/Port   : 12.2.2.3/----
   Inside IP/Port   : 192.168.0.3/----
   Protocol : ----
   VPN instance-name  : ----
   Acl number      : ----
   Netmask  : 255.255.255.255
   Description : ----

 Total :    2
```

配置完成后，PC1和PC2能ping通20.1.2.2。PC3不能ping通Internet上计算机的IP地址。Internet上的PC4能够通过12.2.2.2地址访问内网的PC1，能够通过12.2.2.3地址访问内网的PC3。

测试完成后，删除静态NAT设置，配置NAPT初始化环境。

```
[AR1-GigabitEthernet0/0/1]undo nat static global 12.2.2.2 inside
192.168.0.2
[AR1-GigabitEthernet0/0/1]undo nat static global 12.2.2.3 inside
192.168.0.3
```

9.4 NAPT的实现

本节网络环境如图9-5，假如ISP给企业分配了12.2.2.1、12.2.2.2、12.2.2.3 3个公网地址，12.2.2.1给AR1路由器的GE 0/0/1端口使用，12.2.2.2和12.2.2.3这两个地址给内网计算机做NAPT使用，这就需要定义公网地址池来做NAPT。

创建公网地址池。

```
[AR1]nat address-group 1 ?                                    --指定公网地址池编号1
  IP_ADDR<X.X.X.X>  Start address
[AR1]nat address-group 1 12.2.2.2 12.2.2.3                    --指定开始地址和结束地址
```

如果企业内网有多个网段，那么也许只允许几个网段能够访问Internet。需要通过ACL来定义允许通过NAPT访问Internet的内网网段，在本示例中内网就一个网段。

```
[AR1]acl 2000
[AR1-acl-basic-2000]rule 5 permit source 192.168.0.0 0.0.0.255
[AR1-acl-basic-2000]rule deny
[AR1-acl-basic-2000]quit
```

为AR1上连接Internet的端口GigabitEthernet 0/0/1配置NAPT。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1 ? --指定使用的公网地址池
  no-pat  Not use PAT                                         --如果带no-pat，就是动态NAT
  <cr>    Please press ENTER to execute command
[AR1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1
```

在PC1、PC2、PC3上ping Internet上的PC4，看看是否能通。

9.5 Easy IP的实现

如图9-6所示，企业内网使用私网地址192.168.0.0/24，ISP只给了企业一个公网地址12. 2.2.1/24。在AR1上配置NAPT，允许内网计算机使用AR1路由器上GE 0/0/1端口的公网地址做地址转换以访问Internet。使用路由器端口的公网IP地址做NAPT，该操作称为Easy-IP。

企业内网有多个网段，但也许只允许几个网段能够访问Internet。需要通过ACL来定义允许通过NAPT访问Internet的内网网段，在本示例中内网就一个网段。

```
[AR1]acl 2000
[AR1-acl-basic-2000]rule 5 permit source 192.168.0.0 0.0.0.255
[AR1-acl-basic-2000]rule deny
[AR1-acl-basic-2000]quit
```

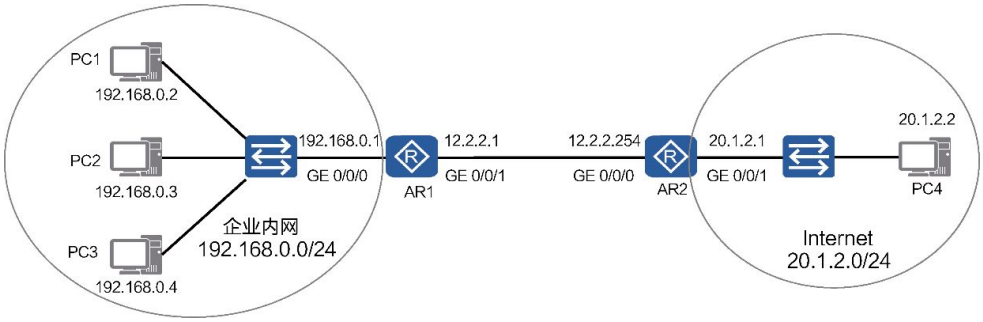


图9-6 使用外网端口地址做NAPT

为AR1上连接Internet的端口GigabitEthernet 0/0/1配置NAPT。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]nat outbound 2000     --指定允许NAPT的ACL
```

9.6　配置端口映射

Internet上的计算机是无法直接访问企业内网（私网IP地址）中的计算机或服务器的。如果打算让Internet上的计算机访问企业内网中的服务器，那么需要在企业连接Internet的路由器上配置端口映射，即NAT Server。该路由器必须有公网IP地址。

如图9-7所示，某公司内网使用的是192.168.0.0/24网段，用AR1路由器连接Internet，有公网IP地址12.2.2.1，该公司内网中的Web服务器需要供Internet上的计算机访问，该公司IT部门的员工下班回家后，需要用远程桌面连接企业内网的Server1和PC3。

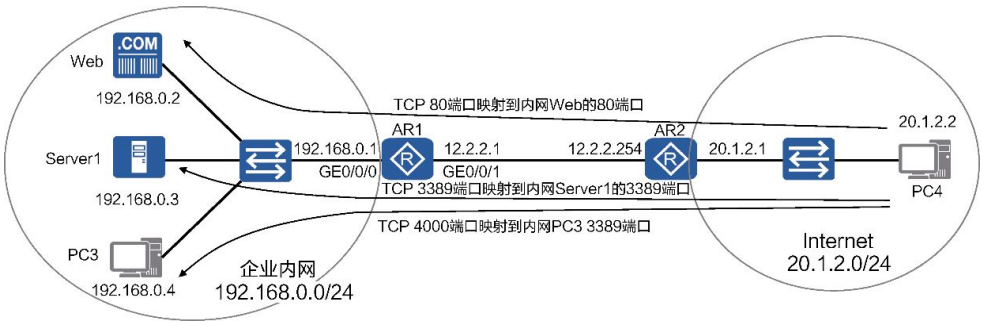


图9-7　配置NAT Server

访问网站使用的是HTTP，该协议默认使用TCP的80端口，将12.2.2.1的TCP的80端口映射到内网192.168.0.2的TCP的80端口。

远程桌面使用的是RDP，该协议默认使用TCP的3389端口，将12.2.2.1的TCP的3389端口映射到内网的192.168.0.3的TCP的3389端口。

TCP的3389端口已经映射到内网的Server1了，使用远程桌面连接PC3时就不能再使用3389端口了，可以将12.2.2.1的TCP的4000端口映射到内网192.168.0.4的3389端口。通过访问12.2.2.1的TCP的4000端口就可以访问PC3的远程桌面（3389端口）。

下面在AR1上配置NAT Server。AR1路由器的GE 0/0/1端口只有一个公网地址12.2.2.1，先配置Easy IP允许内网访问Internet，再配置NAT Server，允许Internet访问内网中的Web服务器、Server1和PC3的远程桌面。

通过ACL定义允许通过NAPT访问Internet的内网，在本示例中内网就一个网段。

```
[AR1]acl 2000
[AR1-acl-basic-2000]rule 5 permit source 192.168.0.0 0.0.0.255
[AR1-acl-basic-2000]rule deny
[AR1-acl-basic-2000]quit
```

在AR1上配置使用GigabitEthernet 0/0/1端口IP地址做网络地址端口转换。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]nat outbound 2000
```

将AR1上的GigabitEthernet 0/0/1端口的地址从TCP的80端口映射到内网的192.168.0.2地址的80端口。

```
[AR1-GigabitEthernet0/0/1]nat server protocol tcp global current-
interface ?
 <0-65535>  Global port of NAT          --可以跟端口号
 ftp   File Transfer Protocol (21)
 pop3    Post Office Protocol v3 (110)
```

```
 smtp    Simple Mail Transport Protocol (25)
 telnet  Telnet (23)
 www     World Wide Web (HTTP, 80)      --www相当于80端口
[AR1-GigabitEthernet0/0/1]nat server protocol tcp global current-
interface www inside 192.168.0.2 www
Warning:The port 80 is well-known port. If you continue it may
cause function failure.
Are you sure to continue?[Y/N]:y
```

将AR1上的GigabitEthernet 0/0/1端口的地址从TCP的3389端口映射到内网的192.168.0.3地址的3389端口。

```
[AR1-GigabitEthernet0/0/1]nat server protocol tcp global current-
interface 3389 inside 192.168.0.3 3389
```

将AR1上的GigabitEthernet 0/0/1端口的地址从TCP的4000端口映射到内网的192.168.0.4地址的3389端口。

```
[AR1-GigabitEthernet0/0/1]nat server protocol tcp global current-
interface 4000 inside 192.168.0.4 3389
```

查看AR1上GigabitEthernet 0/0/1 接口的NAT Server配置。

```
<AR1>display nat server interface GigabitEthernet 0/0/1

 Nat Server Information:
 Interface : GigabitEthernet0/0/1
   Global IP/Port    : current-interface/80(www) (Real IP :
12.2.2.1)
   Inside IP/Port    : 192.168.0.2/80(www)
   Protocol : 6(tcp)
   VPN instance-name  : ----
   Acl number        : ----
   Description : ----

   Global IP/Port    : current-interface/3389 (Real IP : 12.2.2.1)
    Inside IP/Port     : 192.168.0.3/3389
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Description : ----
```

```
    Global IP/Port     : current-interface/4000 (Real IP :
12.2.2.1)
    Inside IP/Port     : 192.168.0.4/3389
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Description : ----

  Total :    3
```

9.7　灵活运用NAPT

NAT和NAPT的产生就是为了解决私网地址访问公网（Internet）的问题，但不能将NAT和NAPT的应用局限于此。下面就介绍NAPT的其他几个应用场景。

9.7.1　“悄悄”在公司网络中接入一个网段

“悄悄”指的是增加一个网段，而无须让网络管理员配置企业路由器以增加到该网段的路由。内网（私网）在公网上是不可见的，在公网的路由器上无须添加到内网的路由。利用这一特点，我们只要有一个能上网的地址，就可以增加一个网段，然后通过该地址来上网。

某学院的网络如图9-8所示，三层交换机LSW1可连接各个教室的交换机，AR1路由器连接Internet。学院内网使用的是10.0.0.0/8私有网段，在AR1路由器上实现NAPT。图9-8还显示了在LSW1和AR1上添加的路由。

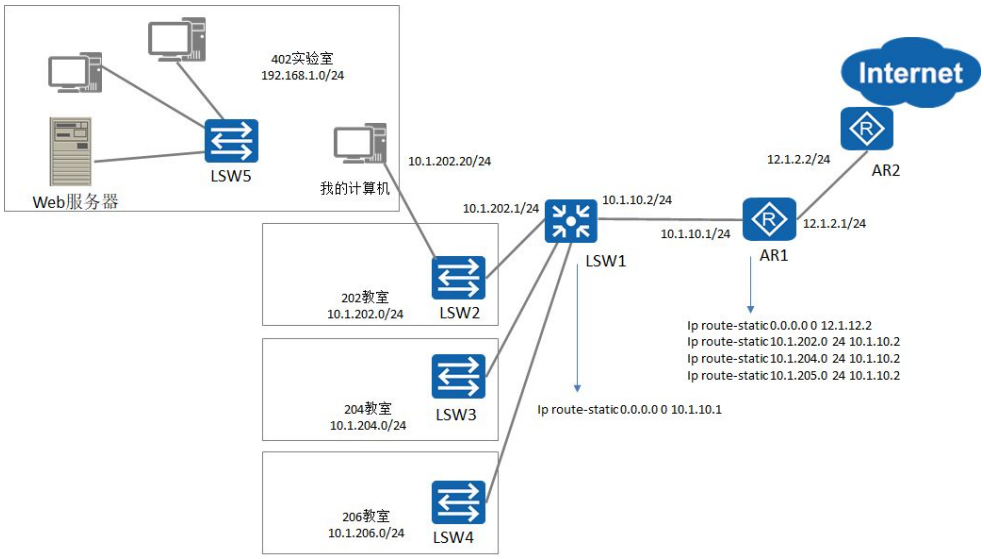


图9-8　学院网络拓扑

如图9-8所示，402实验室是专门为企业用户做培训使用的，使用的网段是192.168.1.0/24，没有接入学院的网络。402实验室在给企业用户做培训时，需要访问Internet。学院的网络管理员拉了一根网线到402实验室，给一台计算机分配了一个地址10.1.202.20，然后将子网掩码设置成255.255.255.0，将网关设置成10.1.202.1，这台计算机就可以通过学院的网络访问Internet了。

参加培训的企业客户提议让402实验室的其他计算机也能够访问Internet。要想在学院的网络中增加一个网段，就需要让网络管理员在LSW1和AR1上增加一个路由。如何在不惊动网络管理员的情况下让402实验室的计算机都能访问Internet呢？

在402实验室有一台闲置的路由器AR3，将连接这台计算机的网线连接到AR3路由器的GE 0/0/0端口，将AR3路由器的GE 0/0/1端口连接到402实验室的LSW5交换机，如图9-9所示。将学院的网络和Internet

看作公网，将402实验室的网络看作私网，配置AR3路由器以实现NAPT。

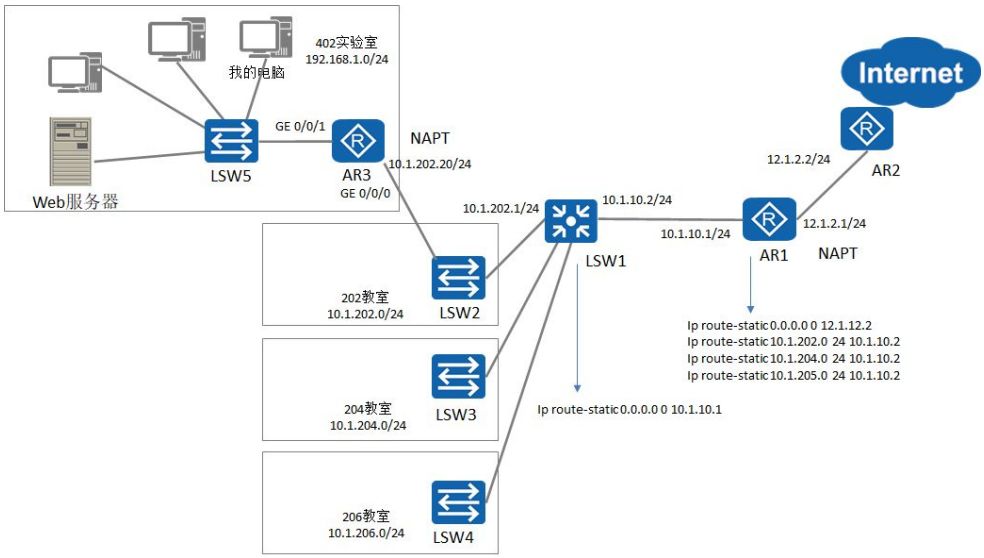


图9-9　在学院网络中增加一个网段

这样402实验室的计算机在访问Internet时需要做两次网络端口地址转换，先经过AR3将源地址替换成10.1.202.20，再经过AR1将数据包的源地址替换成12.1.2.1。

如果Internet上的计算机要访问402实验室的Web服务器，那么需要在AR1上做端口映射，将TCP的80端口映射到10.1.202.20的80端口；接下来在AR3路由器上做端口映射，将TCP的80端口映射到402实验室的Web服务器地址的80端口。

后来学院增加了一台限速设备，每个IP地址访问Internet时的限速为10Mbit/s，402实验室的学生反映访问Internet的速度非常慢。下面分析原因：402实验室的计算机访问Internet时，源地址都被替换成

10.1.202.20了，这就意味着402实验室的所有计算机的上网带宽总共是10Mbit/s。解决办法：删除AR3路由器上的NAPT设置，让网络管理员在学院的网络设备上增加到192.168.1.0/24网段的路由，402实验室的计算机就可以都分配到10Mbit/s带宽了。

9.7.2 实现单向访问

NAPT还有一个特点，内网的计算机能够主动发起对公网的访问，公网的计算机却不能主动发起对内网的访问。可以认为这是单向访问。

某企业的网络如图9-10所示，研发部的网络为了安全，没有和其他网络进行连接，市场部的网络允许访问Internet。现在研发部的计算机需要访问市场部的计算机上的资源，又不想让市场部的计算机访问研发部的计算机上的资源。如何实现呢？

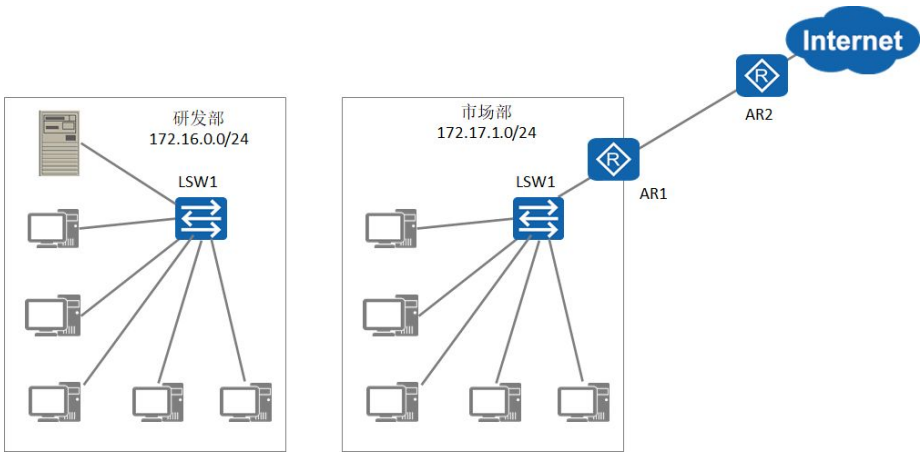


图9-10 某企业的网络拓扑

使用路由器连接研发部和市场部的网络，如图9-11所示。在AR3路由器上配置NAPT，将研发部的网络视为私网，将市场部的网络视为公网。这样研发部就能够访问市场部，而市场部却不能访问研发部。

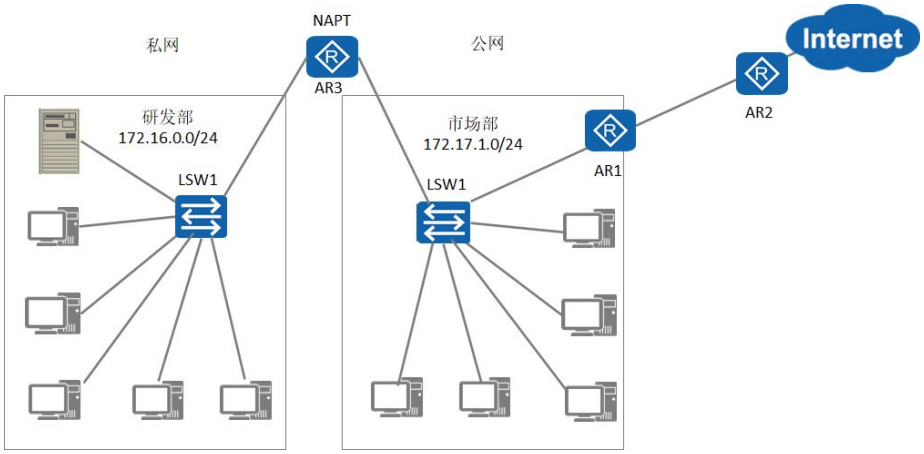


图9-11　配置NAPT以实现内网访问安全

9.8　习题

1．如图9-12所示，为了使主机A能访问公网，且公网用户也能主动访问主机A，此时在路由器R1上应该配置哪种NAT转换模式呢？（　　）

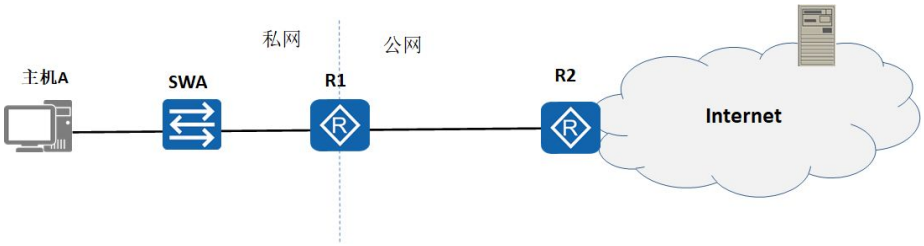


图9-12　通信示意图（一）

A．静态NAT

B．动态NAT

C．Easy-IP

D．NAPT

2．如图9-13所示，RTA使用NAT技术，且通过定义地址池来实现多对多的非NAPT地址转换，使得私网主机能够访问公网。假设地址池中仅有两个公网IP地址，并且已经分配给主机A与B，且做了地址转换。此时若主机C也希望访问公网，则下列描述中正确的是（　　）。

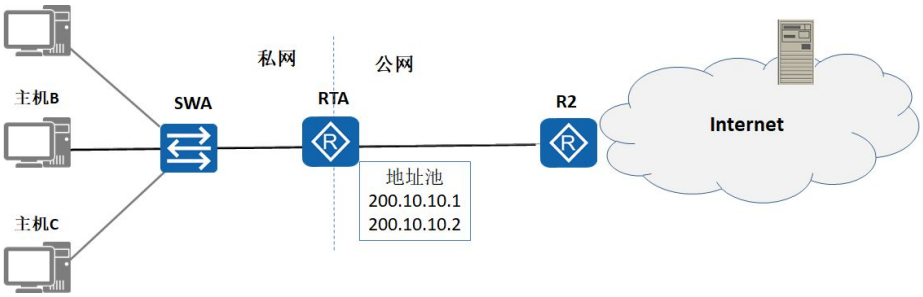


图9-13　通信示意图（二）

A．RTA给主机C分配第一个公网地址，主机A被踢下线

B．RTA给主机C分配最后一个公网地址，主机B被踢下线

C．无法给主机C分配公网地址，不能访问公网

D．所有主机轮流使用公网地址，都可以访问公网

3．下面有关NAT的描述中，正确的是（　　）。（选择3个答案）

A．NAT的全称是网络地址转换，又称为地址翻译

B．NAT通常用来实现私有网络地址与公用网络地址之间的转换

C．当使用具有私有地址的内部网络的主机访问外部公用网络的时候，一定不需要NAT

D．NAT技术为解决IP地址紧张的问题提供了很大的帮助

4．某公司的网络中有50个私有IP地址。网络管理员使用NAT技术接入公网，且该公司仅有一个公网地址可用，则下列哪种NAT转换方式

符合要求？（　　）

A．静态转换

B．动态转换

C．Easy-IP

D．NAPT

5．NAPT允许多个私有IP地址通过不同的端口号映射到同一个公有IP地址。下列关于NAPT中端口号的描述中，正确的是（　　）。

A．必须手动配置端口号和私有地址的对应关系

B．只需要配置端口号的范围

C．不需要做任何关于端口号的配置

D．需要使用ACL分配端口号

第10章　将路由器配置为DHCP服务器

本章内容

- 静态地址和动态地址
- 将华为路由器配置为DHCP服务器
- 抓包分析DHCP分配IP地址的过程
- 跨网段分配IP地址
- 使用接口地址池为直连网段分配地址

本章介绍IP地址的两种配置方式：静态地址分配和动态地址分配，以及这两种方式的适用场景。动态地址方式需要网络中有DHCP服务器，Windows服务器和Linux服务器都可以被配置为DHCP服务器。本章展示将华为路由器配置为DHCP服务器，然后为网络中的计算机分配地址。

路由器打算为多少个网段分配地址，就要创建多少个IP地址池。路由器既可以为直连网段中的计算机分配IP地址，也可以为远程网段（没有直连网段）中的计算机分配IP地址。

如果路由器为直连网段中的计算机分配地址，那么也可以不单独创建IP地址池，而是使用接口地址池为直连网段分配地址。

10.1　静态地址和动态地址

为计算机配置IP地址有两种方式：一种是人工指定IP地址、子网掩码、网关和DNS等配置信息，这种方式获得的IP地址称为静态地址；另一种是使用DHCP服务器为计算机分配IP地址、子网掩码、网关和DNS配置信息，这种方式获得的地址称为动态地址。

适用于静态地址的情况如下所示。

- 计算机在网络中不经常改变位置，比如学校机房，台式机的位置是固定的，这种情况通常使用静态地址。有时为了方便学生访问资源，IP地址还按一定规则进行设置，比如第一排第四列的计算机IP地址设置为192.168.0.14，第三排第二列的计算机IP地址设置为192.168.0.32等。
- 企业的服务器也通常使用固定的IP地址（静态地址），这是为了方便用户使用IP地址访问服务器，比如企业Web服务器、FTP服务器、域控制器、文件服务器、DNS服务器等通常使用静态地址。

适用于动态地址的情况如下所示。

- 网络中的计算机不固定，比如软件学院，每个教室一个网段，202教室的网络是10.7.202.0/24网段，204教室的网络是10.7.204.0/24网段。学生从202教室下课后再去204教室上课，便携式计算机就要更改IP地址了。如果让学生自己更改IP地址（静态地址），那么设置的地址有可能已经被其他学生的便携式计算机占用了。人工为移动设备指定地址不仅麻烦，而且指定的地址

还容易发生冲突。如果使用DHCP服务器统一分配地址，就不会产生冲突。

- 通过Wi-Fi联网的设备，地址通常也是由DHCP服务器自动分配的。通过Wi-Fi联网本来就是为了方便，如果连上Wi-Fi后，还要设置IP地址、子网掩码、网关和DNS才能上网，那就不方便了。

10.2　将华为路由器配置为DHCP服务器

如图10-1所示，某企业有3个部门，销售部的网络使用192.168.1.0/24网段、市场部的网络使用192.168.2.0/24网段、研发部的网络使用172.16.5.0/24网段。现在要将AR1路由器配置为DHCP服务器，来为这3个部门的计算机分配IP地址。

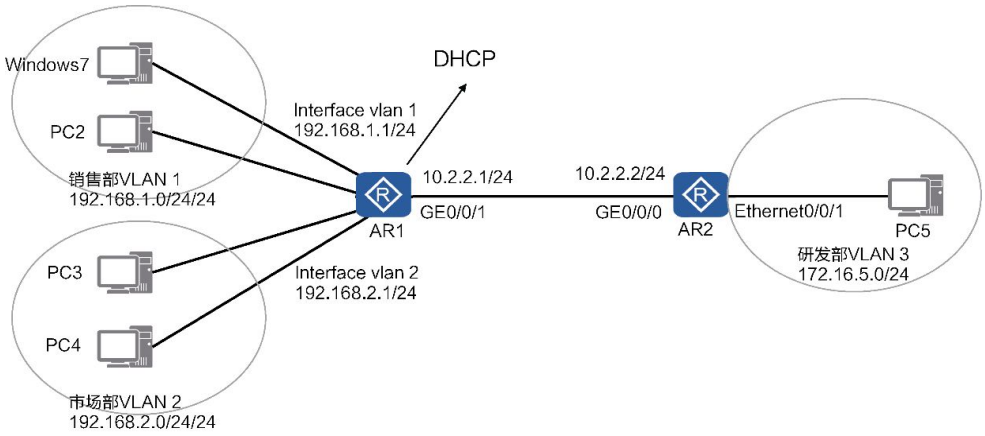


图10-1　DHCP网络拓扑

在AR1上为销售部创建地址池vlan1，vlan1是地址池的名称，地址池名称可以随便指定。

```
[AR1]dhcp enable                                          --全局启用DHCP服务
[AR1]ip pool vlan1                                        --为vlan 1创建地址池
[AR1-ip-pool-vlan1]network 192.168.1.0 mask 24  --指定地址池所在的网段
[AR1-ip-pool-vlan1]gateway-list 192.168.1.1     --指定该网段的网关
[AR1-ip-pool-vlan1]dns-list 8.8.8.8             --指定DNS服务器
[AR1-ip-pool-vlan1]dns-list 222.222.222.222     --指定第二个DNS服务器
[AR1-ip-pool-vlan1]lease day 0 hour 8 minute 0  --地址租约，允许客户端使用多长时间
[AR1-ip-pool-vlan1]excluded-ip-address 192.168.1.1 192.168.1.10 --指定排除的地址范围
Error:The gateway cannot be excluded.           --不能包括网关
```

```
[AR1-ip-pool-vlan1]excluded-ip-address 192.168.1.2 192.168.1.10 --
指定排除的地址范围
[AR1-ip-pool-vlan1]excluded-ip-address 192.168.1.50 192.168.1.60 -
-指定排除的地址范围
[AR1-ip-pool-vlan1]display this                    --显示地址池的配置
[V200R003C00]
#
ip pool vlan1
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
 excluded-ip-address 192.168.1.2 192.168.1.10
 excluded-ip-address 192.168.1.50 192.168.1.60
 lease day 0 hour 8 minute 0
 dns-list 8.8.8.8 222.222.222.222
#
Return
```

配置Vlanif 1接口从全局地址池选择地址。以上创建的vlan1地址池是全局（global）地址池。

```
[AR1]interface Vlanif 1
[AR1-Vlanif1]dhcp select global
```

一个网段只能创建一个地址池，如果该网段中有些地址已经被占用，就要在该地址池中排除，避免DHCP分配的地址和其他计算机冲突。DHCP分配给客户端的IP地址等配置信息是有时间限制的（租约时间），对于网络中计算机变换频繁的情况，租约时间设置得短一些；如果网络中的计算机相对稳定，租约时间设置得长一点。软件学院的学生2小时就有可能更换教室听课，可把租约时间设置成2小时。通常情况下，客户端在租约时间过去一半就会自动找到DHCP服务器续约。如果到期了，客户端没有找DHCP服务器续约，DHCP就认为该客户端已经不在网络中，该地址就被收回，以后就可以分配给其他计算机了。

为市场部创建地址池。

```
[AR1]ip pool vlan2
[AR1-ip-pool-vlan2]network 192.168.2.0 mask 24
[AR1-ip-pool-vlan2]gateway-list 192.168.2.1
[AR1-ip-pool-vlan2]dns-list 114.114.114.114
[AR1-ip-pool-vlan2]lease day 0 hour 2 minute 0
[AR1-ip-pool-vlan2]quit
```

配置Vlanif 2接口以从全局地址池选择地址。

```
[AR1]interface Vlanif 2
[AR1-Vlanif2]dhcp select global
```

输入display ip pool以显示定义的地址池。

```
<AR1>display ip pool
 ------------------------------------------------------------------
------
 Pool-name      : vlan1
 Pool-No        : 0
 Position       : Local           Status           : Unlocked
 Gateway-0      : 192.168.1.1
 Mask           : 255.255.255.0
 VPN instance   : --

 ------------------------------------------------------------------
------
 Pool-name      : vlan2
 Pool-No        : 1
 Position       : Local           Status           : Unlocked
 Gateway-0      : 192.168.2.1
 Mask           : 255.255.255.0
 VPN instance   : --

 IP address Statistic
  Total      :506
  Used       :4          Idle        :482
  Expired    :0          Conflict    :0          Disable   :20
```

在Windows 7上运行抓包工具，将IP地址设置成自动获得，这能够捕获请求IP地址的过程。可以看到DHCP客户端和DHCP服务器交互的4个数据包，也就是DHCP协议的工作过程，如图10-2所示。

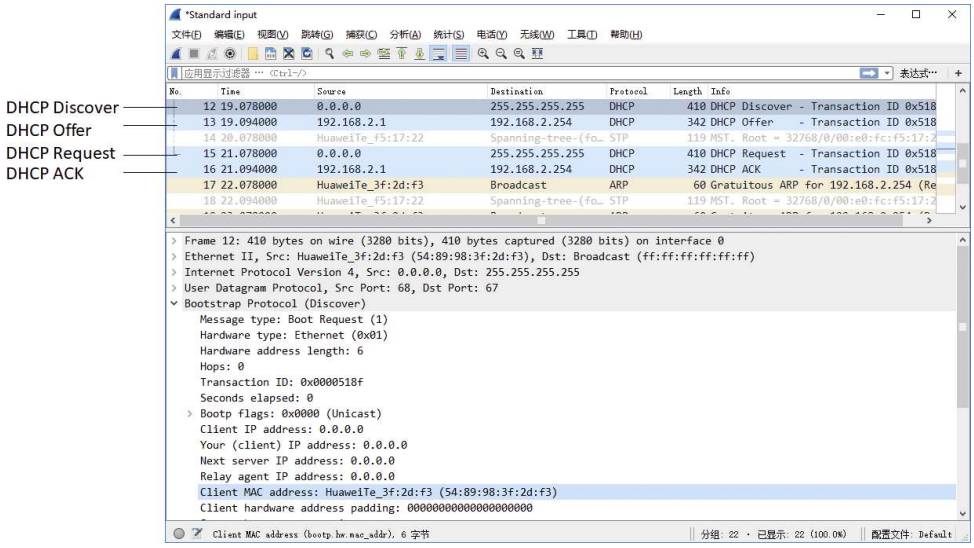


图10-2　DHCP的工作过程

DHCP通过4个步骤将IP地址信息以租约的方式提供给DHCP客户端。这4个步骤分别以DHCP数据包的类型命名。

步骤1：DHCP Discover（DHCP发现）。

DHCP客户端通过向网络广播一个DHCP Discover数据包来发现可用的DHCP服务器。

将IP地址设置为自动获得的计算机就是DHCP客户端，它不知道网络中谁是DHCP服务器，自己也没地址，DHCP客户端就发送广播包来请求地址，网络中的设备都能收到该请求。广播包的源IP地址为0.0.0.0，目标IP地址为255.255.255.255。

步骤2：DHCP Offer（DHCP提供）。

DHCP服务器通过向网络广播一个DHCP Offer数据包来应答客户端的请求。

当DHCP服务器接收到DHCP客户端广播的DHCP Discover数据包后，网络中的所有DHCP服务器都会向网络广播一个DHCP Offer数据包。所谓DHCP Offer数据包，就是DHCP服务器用来将IP地址提供给DHCP客户端的信息。

步骤3：DHCP Request（DHCP选择）。

DHCP客户端向网络广播一个DHCP Request数据包来选择多个服务器提供的IP地址。

DHCP客户端接收到服务器的DHCP Offer数据包后，会向网络广播一个DHCP Request数据包以接受分配。DHCP Request数据包包含了为客户端提供租约的DHCP服务器的标识，这样其他DHCP服务器收到这个数据包后，就会撤销对这个客户端的分配，而将本该分配的IP地址收回用于响应其他客户端的租约请求。

步骤4：DHCP ACK （DHCP确认）。

被选择的DHCP服务器向网络广播一个DHCP ACK数据包，用以确认客户端的选择。

在DHCP服务器接收到客户端广播的DHCP Request数据包后，随即向网络广播一个DHCP ACK数据包。所谓DHCP ACK数据包，就是DHCP服

务器发给DHCP客户端的用以确认IP地址租约成功生成的信息。此信息包含该IP地址的有效租约和其他的IP配置信息。

显示地址池vlan1的地址租约使用情况。

```
<AR1>display ip pool name vlan1 used
 Pool-name      : vlan1
 Pool-No        : 0
 Lease          : 0 Days 8 Hours 0 Minutes
 Domain-name    : -
 DNS-server0    : 8.8.8.8
 DNS-server1    : 222.222.222.222
 NBNS-server0   : -
 Netbios-type   : -
 Position       : Local           Status           : Unlocked
 Gateway-0      : 192.168.1.1
 Mask           : 255.255.255.0
 VPN instance   : --
-------------------------------------------------------------------------
-----------
    Start         End     Total  Used  Idle(Expired)  Conflict
Disable
-------------------------------------------------------------------------
-----------
  192.168.1.1   192.168.1.254   253     2     231(0)        0
20
-------------------------------------------------------------------------
-----------

 Network section :
 -------------------------------------------------------------------------
---------
 Index    IP       MAC              Lease   Status
 -------------------------------------------------------------------------
---------
  252   192.168.1.253    5489-9851-4a95      335   Used  --租约，有
客户端MAC地址
  253   192.168.1.254    5489-9831-72f6      344   Used  --租约，有
客户端MAC地址
 -------------------------------------------------------------------------
---------
```

10.3　跨网段分配IP地址

在AR1路由器上创建地址池remoteNet，从而为研发部的计算机分配地址。研发部的网络没有和AR1路由器直连，AR1路由器收不到研发部的计算机发送的DHCP发现数据包，路由器隔绝广播。这就需要配置AR2路由器的Vlanif 1接口，启用DHCP中继功能，然后将收到的DHCP发现数据包转换成定向DHCP发现数据包，其中目标地址为10.2.2.1，源地址为接口Vlanif 1的地址172.16.5.1。AR1路由器一旦收到这样的数据包，就知道这是来自172.16.5.0/24网段的请求，于是就从remoteNet地址池中选择一个IP地址提供给PC5，如图10-3所示。完成本实验的前提是确保这几个网络畅通。

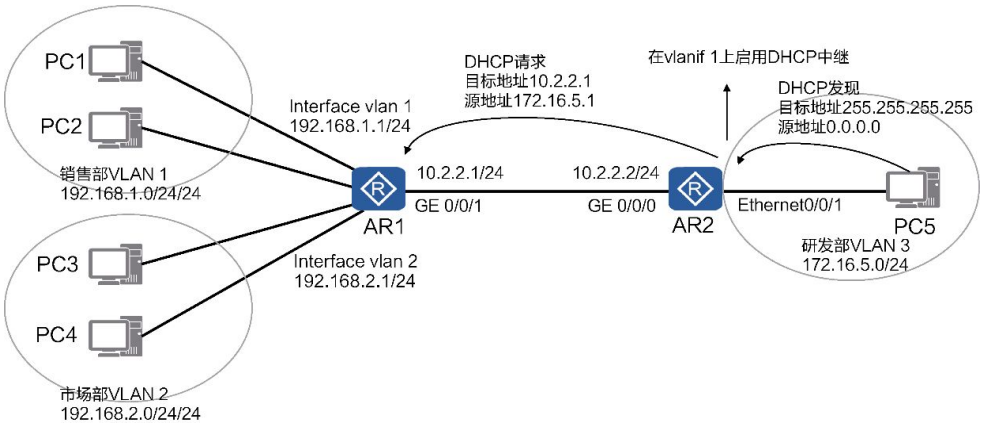


图10-3　跨网段分配IP地址的拓扑图

下面就在AR1上为研发部的网络创建地址池remoteNet。远程网段的地址池必须设置网关。

```
[AR1]ip pool remoteNet
[AR1-ip-pool-remoteNet]network 172.16.5.0 mask 24
[AR1-ip-pool-remoteNet]gateway-list 172.16.5.1              --必须设置
```

```
网关
[AR1-ip-pool-remoteNet]dns-list 8.8.8.8
[AR1-ip-pool-remoteNet]lease day 0 hour 2 minute 0
[AR1-ip-pool-remoteNet]quit
```

配置AR1的GE 0/0/0接口从全局地址池选择地址。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]dhcp select global
[AR1-GigabitEthernet0/0/0]quit
```

在AR2路由器上启用DHCP功能，配置AR2路由器的Vlanif 1接口，启用DHCP中继功能，指明DHCP服务器的地址。

```
[AR2]dhcp enable
[AR2]interface Vlanif 1
[AR2-Vlanif1]dhcp select relay
[AR2-Vlanif1]dhcp relay server-ip 10.2.2.1
```

将PC5的地址设置成DHCP动态分配，输入ipconfig以查看获得的IP地址，并验证跨网段分配。如果不成功，检查AR1和AR2路由器上的路由表。要确保网络畅通，DHCP才能跨网段分配IP地址。

```
PC>ipconfig
Link local IPv6 address...........: fe80::5689:98ff:fe61:65d
IPv6 address......................: :: / 128
IPv6 gateway......................: ::
IPv4 address......................: 172.16.5.254
Subnet mask.......................: 255.255.255.0
Gateway...........................: 172.16.5.1
Physical address..................: 54-89-98-61-06-5D
DNS server........................: 8.8.8.8
```

10.4　使用接口地址池为直连网段分配地址

以上操作将华为路由器配置为DHCP服务器，一个网段创建一个地址池，还为地址池指定了网段和子网掩码。如果路由器为直连网段分配地址，那么可以不用创建地址池。既然已经为路由器接口配置了地址和子网掩码，那么可以使用接口所在的网段作为地址池的网段和子网掩码。

如图10-4所示，AR1路由器连接两个网段192.168.1.0/24和192.168.2.0/24。要求配置AR1路由器为这两个网段分配IP地址。

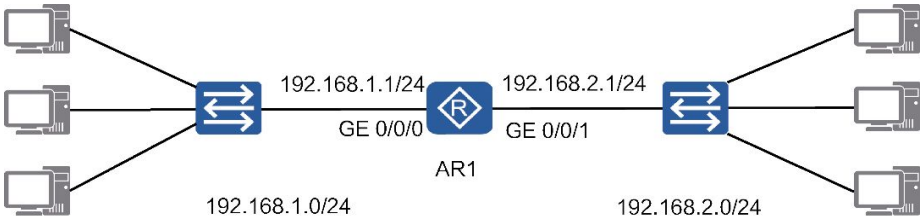


图10-4　使用接口地址池为直连网段分配地址的拓扑图

配置AR1的GigabitEthernet 0/0/0和GigabitEthernet 0/0/1接口地址。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ip address 192.168.1.1 24
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]ip address 192.168.2.1 24
[AR1-GigabitEthernet0/0/1]
```

启用DHCP服务，配置GigabitEthernet 0/0/0接口从接口地址池选择地址。

```
 [AR1]dhcp enable                                          --全局启用DHCP服
务
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]dhcp select interface     --从接口地址池选
择地址
[AR1-GigabitEthernet0/0/0]dhcp server dns-list 114.114.114.114
[AR1-GigabitEthernet0/0/0]dhcp server ?             --可以看到全部配
置项
 dns-list       Configure DNS servers
 domain-name        Configure domain name
 excluded-ip-address  Mark disable IP addresses
 ……
 lease        Configure the lease of the IP pool
[AR1-GigabitEthernet0/0/0]dhcp server excluded-ip-address
192.168.1.2 192.168.1.20
                                                          --排除地址
```

配置GigabitEthernet 0/0/1接口从接口地址池选择地址。

```
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]dhcp select interface
[AR1-GigabitEthernet0/0/1]dhcp server dns-list 8.8.8.8
[AR1-GigabitEthernet0/0/1]dhcp server lease day 0 hour 4 minute 0
```

10.5　习题

1．管理员在网络中部署了一台DHCP服务器之后，发现部分主机获取到非该DHCP服务器指定的地址，可能的原因有哪些？（　　）（选择3个答案）

A．网络中存在另一台工作效率更高的DHCP服务器。

B．部分主机无法与该DHCP服务器正常通信，这些主机客户端系统自动生成了169.254.0.0范围内的地址

C．部分主机无法与该DHCP服务器正常通信，这些主机客户端系统自动生成了127.254.0.0范围内的地址

D．DHCP服务器的地址池已经全部分配完毕

2．管理员在配置DHCP服务器时，下面哪条命令配置的租期时间最短？（　　）

A．dhcp select

B．lease day 1

C．lease 24

D．lease 0

3．主机从DHCP服务器A获取到IP地址后进行了重启，则重启事件会向DHCP服务器A发送下面哪种消息？（　　）

A．DHCP Discover

B．DHCP Request

C．DHCP Offer

D．DHCP ACK

4．如图10-5所示，在RA路由器上启用DHCP服务，为192.168.3.0/24网段创建地址池，需要在RB路由器上做哪些配置，才能使PC2从RA路由器获得IP地址？（　　）

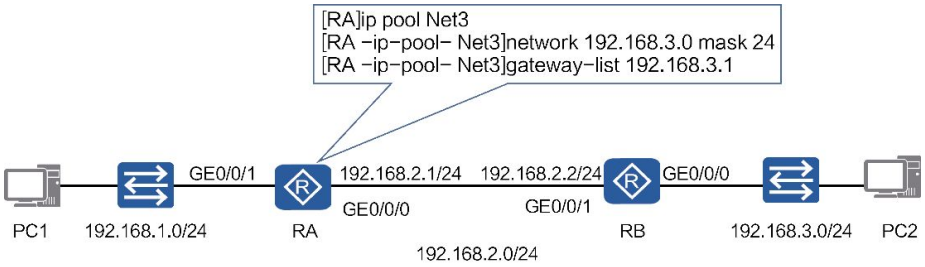


图10-5　通信示意图

A．[RB]dhcp enable

[RB]interface GigabitEthernet 0/0/0

[RB-GigabitEthernet 0/0/0]dhcp select global

B．[RB]dhcp enable

[RB]interface GigabitEthernet 0/0/0

[RB-GigabitEthernet 0/0/0]dhcp select relay

[RB-GigabitEthernet 0/0/0]dhcp relay server-ip 192.168.2.1

C. [RB]dhcp enable

[RB]interface GigabitEthernet 0/0/1

[RB-GigabitEthernet 0/0/0]dhcp select relay

[RB-GigabitEthernet 0/0/0]dhcp relay server-ip 192.168.2.1

D. [RB]interface GigabitEthernet 0/0/0

[RB-GigabitEthernet 0/0/0]dhcp select relay

[RB-GigabitEthernet 0/0/0]dhcp relay server-ip 192.168.2.1

5. 使用动态主机配置协议DHCP分配IP地址有哪些优点？（　　）（多选）

A. 可以实现IP地址重复利用

B. 避免IP地址冲突

C. 工作量大且不好管理

D. 配置信息发生变化（如DNS），只需要管理员在DHCP服务器上修改，方便统一管理

6. 以下哪条命令可以开启路由器接口的DHCP中继功能？（　　）

A. dhcp select server

B. dhcp select global

C. dhcp select interface

D. dhcp select relay

第11章　IPv6

本章内容

- IPv6的优势
- IPv6地址
- 自动配置IPv6地址
- IPv6路由

本章介绍IPv6协议相对于IPv4有哪些改进，IPv6网络层协议相对于IPv4网络层协议有哪些变化，以及ICMPv6协议有哪些功能上的扩展。

IPv6地址由128位二进制数构成，解决了IPv4公网地址紧张的问题。本章讲解IPv6地址的格式、简写规则及分类。

计算机的IPv6地址可以人工指定静态地址，也可以设置为自动获取，自动获取分为“无状态自动配置”和“有状态自动配置”，本章介绍这两种自动配置如何实现。

IPv6的功能和IPv4一样，都是为数据包选择转发路径。网络要想畅通，需要给路由器添加静态路由，或使用动态路由协议学习到各个网段的路由。本章展示IPv6的静态路由配置和动态路由OSPFv3配置。

11.1 IPv6的优势

与IPv4相比，IPv6具有以下几个优势。

- 近乎无限的地址空间：与IPv4相比，这是最明显的好处。IPv6地址是由128位（bit）构成。单从数量级来说，IPv6所拥有的地址容量是IPv4的约2×10^{96}倍。这使得海量终端同时在线、统一编址管理变为可能，它为万物互联提供了强有力的支撑。
- 层次化的地址结构：正因为有了近乎无限的地址空间，IPv6在地址规划时就可以根据使用场景划分各种地址段。IPv6严格要求单播IPv6地址段的连续性，这便于IPv6路由聚合，缩小IPv6地址表规模。
- 即插即用：任何计算机或者终端要获取网络资源，传输数据，都必须有明确的IP地址。传统的分配IP地址方式是手动或者DHCP自动获取。除了上述两个方式外，IPv6还支持无状态地址自动配置（Stateless Address Autoconfiguration，SLAAC）。
- 端到端网络的完整性：大面积使用NAT技术的IPv4网络，从根本上破坏了端到端连接的完整性。使用IPv6之后，上网将不再需要NAT网络设备，上网行为管理、网络监管等将变得简单。
- 安全性得到增强：IPsec（Internet Protocol Security，Internet协议安全协议）最初是为IPv6设计的，基于IPv6的各种协议报文（路由协议、邻居发现等）都可以端到端地加密，当然该功能目前的应用并不多。而IPv6的数据包文安全性与IPv4+IPsec的能力基本相同。
- 可扩展性强：IPv6的扩展首部并不是网络层首部的一部分，但是在必要的时候，这些扩展首部插在IPv6基本首部和有效载荷之

间，能够协助IPv6完成加密功能、移动功能、最优路径选路、QoS等，并可提高报文转发效率。

- 移动性改善：当一个用户从一个网段移动到另外一个网段时，传统的网络会产生经典的“三角式路由”。在IPv6网络中，这种移动设备的通信，可不再经过原“三角式路由”而直接进行路由转发，降低了流量转发的成本，提升了网络性能和可靠性。
- QoS可得到进一步增强：IPv6保留了IPv4所有的QoS属性，额外定义了20字节的流标签字段，可为应用程序或者终端所用。针对特殊的服务和数据流，IPv6可分配特定的资源。目前该机制并没有得到充分的开发和应用。

图11-1是对TCP/IPv4协议栈和TCP/IPv6协议栈的比较。

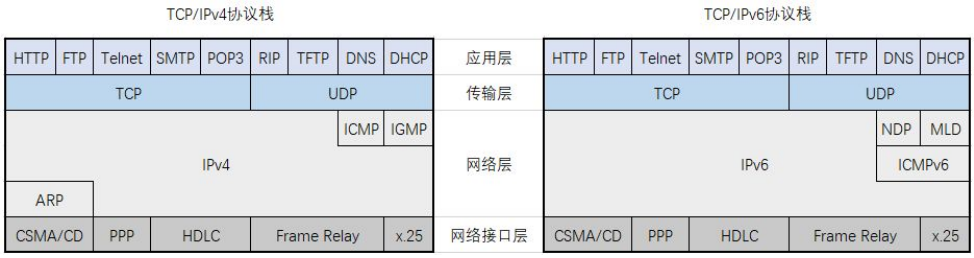


图11-1　TCP/IPv4协议栈和TCP/IPv6协议栈

可以看到，TCP/IPv6协议栈与TCP/IPv4协议栈相比，只是网络层发生了变化，实现的功能是相同的。TCP/IPv6协议栈的网络层没有ARP和IGMP，对ICMP的功能做了很大的扩展，IPv4协议栈中ARP的功能和IGMP的组播成员管理功能也被嵌入到ICMPv6中，分别是邻居发现协议（Neighbor Discovery Protocol，NDP）和组播侦听器发现（Multicast Listener Discovery，MLD）协议。

IPv6网络层的核心协议的功能如下。

- Internet控制消息协议IPv6版（ICMPv6）：用来取代ICMP，测试网络是否畅通，报告错误和其他信息以帮助判断网络故障。
- 邻居发现协议（NDP）：NDP取代了ARP，用于管理相邻IPv6结点间的交互，包括自动配置地址以及将下一跳IPv6地址解析为MAC地址。
- 组播侦听器发现（MLD）协议：MLD取代了IGMP，用于管理IPv6组播组成员的身份。

11.1.1　IPv6的基本首部

IPv6数据包在基本首部（base header）的后面允许有零个或多个扩展首部（extension header)，再后面是数据，如图11-2所示。但请注意，所有的扩展首部都不属于IPv6数据包的首部。所有的扩展首部和数据合起来叫作数据包的有效载荷（payload）或净负荷。

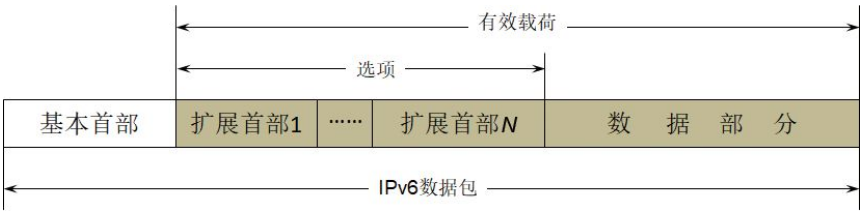


图11-2　基本首部和扩展首部

图11-3是IPv6数据包的基本首部。在基本首部后面是有效载荷，它包括传输层的数据和可能选用的扩展首部。

与IPv4相比，IPv6对首部中的某些字段进行了如下的更改。

- 取消了首部长度字段，因为它的首部长度是固定的（40字节）。

- 取消了服务类型字段，因为优先级和流标号字段合起来实现了服务类型字段的功能。
- 取消了总长度字段，改用有效载荷长度字段。
- 取消了标识、标志和片偏移字段，因为这些功能已包含在分片扩展首部中。
- TTL字段改名为跳数限制字段，但作用是一样的（名称与作用更加一致）。
- 取消了协议字段，改用下一个首部字段。
- 取消了检验和字段，这样就加快了路由器处理数据包的速度。差错检验交给了数据链路层和传输层，在数据链路层就丢弃检测出有差错的帧。在传输层，当使用UDP时，若检测出有差错的用户数据包就丢弃。当使用TCP时，若检测出有差错的报文段就重传，直到正确传送到目的进程为止。
- 取消了选项字段，而用扩展首部来实现选项功能。

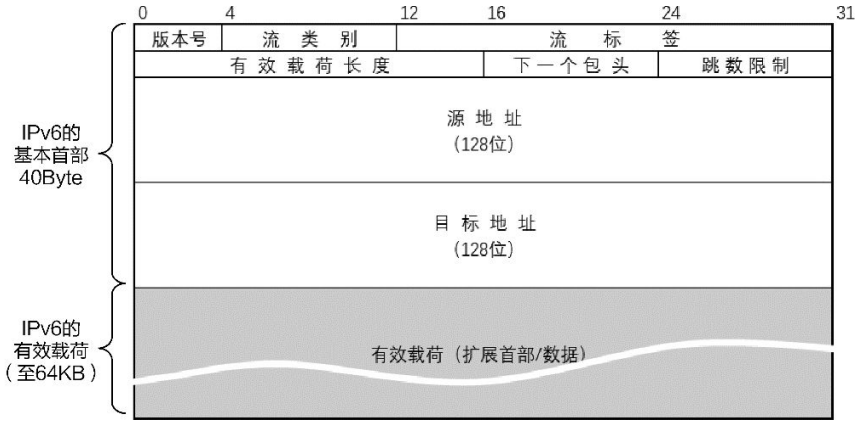


图11-3　IPv6数据包基本首部

由于把网络首部中不必要的功能取消了，因此IPv6首部的字段数减少到只有8个（虽然首部长度增加了一倍）。

下面解释IPv6基本首部中各字段的作用。

- 版本号：长度为4 bit。对于IPv6，该值为6。
- 流类别：长度为8 bit。等同于IPv4中的QoS字段，表示IPv6数据包的类或优先级，主要应用于QoS。
- 流标签：长度为20 bit。IPv6中的新增字段，用于区分实时流量，不同的流标签+源地址可以唯一确定一条数据流，中间网络设备可以根据这些信息更加高效率地区分数据流。
- 有效载荷长度：长度为16 bit。有效载荷是指紧跟IPv6首部的数据包的其他部分（即扩展首部和上层协议数据单元）。
- 下一个首部：长度为8 bit。该字段定义紧跟在IPv6首部后面的第一个扩展首部（如果存在）的类型后，或者上层协议数据单元中的协议类型（类似于IPv4的Protocol字段）后。
- 跳数限制：长度为8 bit。该字段类似于IPv4中的Time to Live字段，它定义了IP数据包所能经过的最大跳数。每经过一个路由器，该数值减去1，当该字段的值为0时，数据包将被丢弃。
- 源地址：长度为128 bit，表示发送方的地址。
- 目的地址：长度为128 bit，表示接收方的地址。

11.1.2　IPv6的扩展首部

IPv4的数据包如果在其首部中使用了选项，那么沿数据包传送的路径上的每一个路由器都必须对这些选项一一进行检查，这就降低了路由器处理数据包的速度。然而实际上很多的选项在途经的路由器上是不需要检查的（因为不需要使用这些选项的信息）。

IPv6把原来IPv4首部中选项的功能都放在扩展首部中，并把扩展首部留给路径两端的源点和终点的计算机来处理，而数据包途中经过的路由器都不处理这些扩展首部（只有一个首部例外，即逐跳选项扩

展首部），这样就大大提高了路由器的处理效率。RFC2460定义了以下6种扩展首部，当超过一种扩展首部被用在同一个IPv6报文里时，扩展首部必须按照下列顺序出现。

- 逐跳选项首部：主要用于为在传送路径上的每跳转发指定发送参数，传送路径上的每台中间节点都要读取并处理该字段。
- 目的选项首部：携带了一些只有目的节点才会处理的信息。
- 路由首部：IPv6源节点用来强制数据包经过特定的设备。
- 分片首部：当报文长度超过最大传输单元（Maximum Transmission Unit，MTU）时就需要将报文分片发送，而在IPv6中，分片发送使用的是分片首部。
- 认证首部（AH）：该首部由IPsec使用，提供认证、数据完整性以及重放保护。
- 封装安全有效载荷首部（ESP）：该首部由IPsec使用，提供认证、数据完整性、重放保护和IPv6数据包的保密。

IPv6基本首部的“下一个首部”字段，用来指明基本首部后面的数据应交付IP层上面的哪一个高层协议。比如，6表示应交付给传输层的TCP，17表示应交付给传输层的UDP，58表示应交付给ICMPv6。

表11-1列出了规范中定义的所有扩展首部对应的“下一个首部”的取值。

表11-1　扩展首部对应的首部值

对应扩展首部类型	下一个首部值

对应扩展首部类型	下一个首部值
逐跳选项首部	0
目的选项首部	60
路由选择首部	43
分片首部	44
认证首部	51
封装安全有效载荷首部	50
无下一个扩展首部	59

每一个扩展首部都由若干个字段组成，它们的长度也各不同。但所有扩展首部的第一个字段都是8位的“下一个首部”字段。此字段的值指出了该扩展首部后面的字段是什么。如图11-4所示，IPv6数据包中扩展首部包括路由选择首部、分片首部、最后是TCP首部。

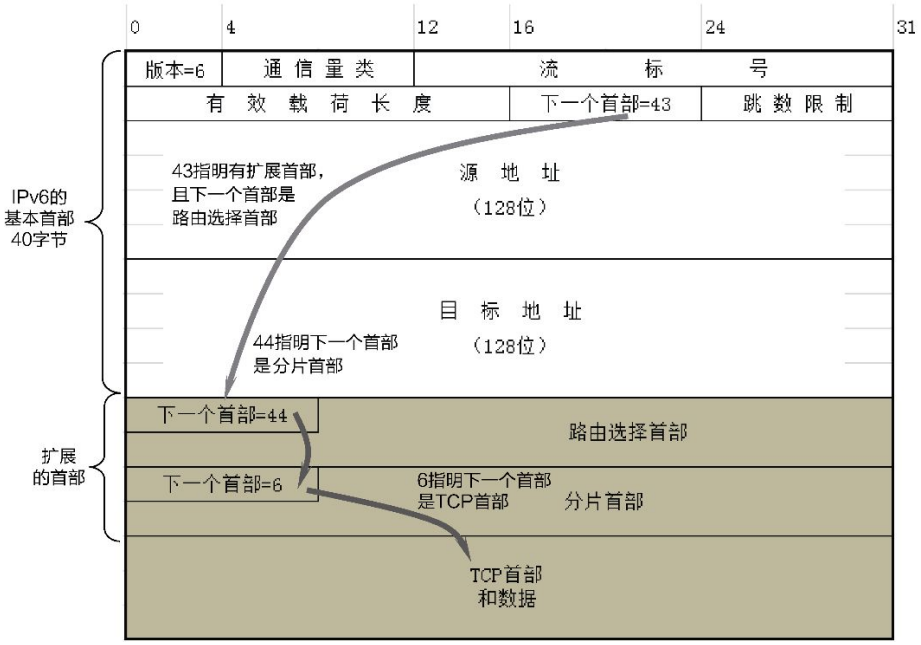

0
4
12
16
24
31
版本=6
通 信 量 类
流 标 号
有 效 载 荷 长 度
下一个首部=43
跳 数 限 制
源 地 址
(128位)
目 标 地 址
(128位)
IPv6的
基本首部
40字节
43指明有扩展首部，
且下一个首部是
路由选择首部
44指明下一个首部
是分片首部
下一个首部=44
路由选择首部
扩展
的首部
下一个首部=6
6指明下一个首部
是TCP首部
分片首部
TCP首部
和数据

图11-4　扩展首部

11.2　IPv6地址

11.2.1　IPv6地址格式

在Internet发展初期，IPv4以其协议简单、易于实现、互操作性好的优势而得到快速发展。然而，随着Internet的迅猛发展，IPv4地址不足等设计缺陷也日益明显。IPv4理论上能够提供的地址数量是43亿，但是由于地址分配机制等，实际可使用的数量还远远达不到43亿。Internet的迅猛发展令人始料未及，同时也带来地址短缺的问题。针对这一问题，曾先后出现过几种解决方案，比如CIDR和NAT。但是CIDR和NAT都有各自的弊端和不能解决的问题，在这样的情况下，IPv6的应用和推广便显得越来越急迫。

IPv6是Internet工程任务组（IETF）设计的一套规范，是网络层协议的第二代标准协议，也是IPv4（Internet Protocol version 4）的升级版本。IPv6与IPv4最显著的区别是，IPv4地址采用32位，而IPv6地址采用128位。128位的IPv6地址可以划分更多地址层级、拥有更广阔的地址分配空间，并支持地址自动配置。IPv4地址空间已经消耗殆尽，近乎无限的地址空间是IPv6的最大优势，如图11-5所示。

版本	长度	地址数量
IPv4	32位	4294967296
IPv6	128位	340282366920938463374607431768211456

图11-5　IPv4和IPv6地址数量对比

如图11-6所示，IPv6地址的长度为128位，用于标识一个或一组接口。IPv6地址通常写作××××：××××：××××：××××：××××：××××：××××：××××，其中××××是4个十六进制数，等同于一个16位的二进制数；八组××××共同组成了一个128位的IPv6地址。一个IPv6地址由IPv6地址前缀和接口ID组成，IPv6地址前缀用来标识IPv6网络，接口ID用来标识接口。

由于IPv6地址的长度为128位，因此书写时会非常不方便。此外，IPv6地址的巨大地址空间使得地址中往往会包含多个0。为了应对这种情况，IPv6提供了压缩方式来简化地址的书写，压缩规则如下所示。

- 每16位中的前导0可以省略。
- 地址中包含的连续两个或多个均为0的组，可以用双冒号“::”来代替。需要注意的是，在一个IPv6地址中只能使用一次双冒号“::”，否则，设备将压缩后的地址恢复成128位时，无法确定每段中0的个数，如图11-7所示。

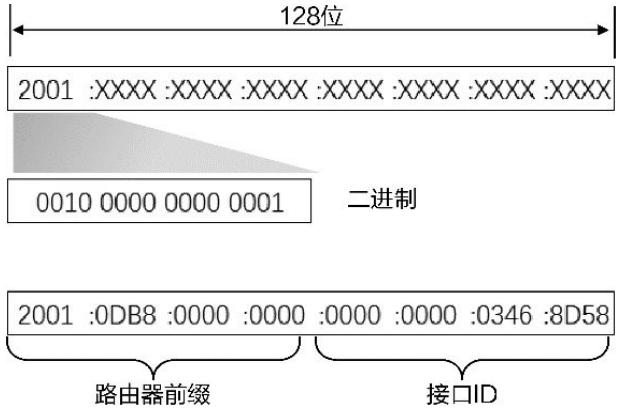


图11-6　IPv6地址的组成

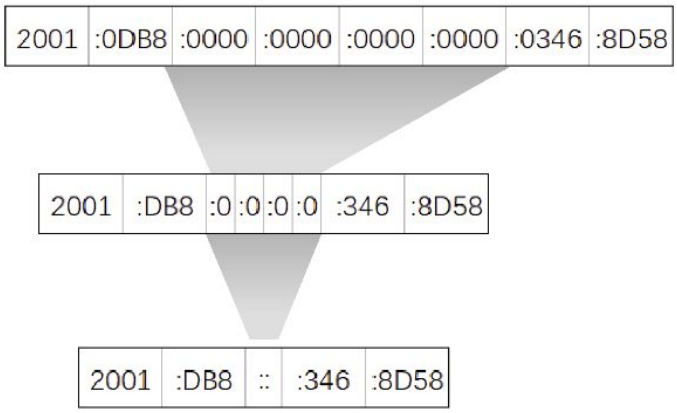


图11-7　IPv6地址的简化表示

本示例展示了如何利用压缩规则对IPv6地址进行简化表示。

IPv6地址分为IPv6地址前缀和接口ID，子网掩码使用前缀长度的方式标识。表示形式是：IPv6地址/前缀长度，其中“前缀长度”是一个十进制数，表示该地址的前多少位是地址前缀。例如FOOD:4598:7304:3210:FEDC:BA98:7654:3210，其地址前缀是64位，可以表示为FOOD: 4598:7304:3210:FEDC:BA98:7654:3210/64。

11.2.2　IPv6地址分类

根据IPv6地址前缀，可将IPv6地址分为单播（Unicast）地址、组播（Multicast）地址和任播（Anycast）地址，如图11-8所示。单播地址又分为全球单播地址、唯一本地地址、链路本地地址、特殊地址和其他单播地址。IPv6没有定义广播地址（Broadcast Address）。在IPv6网络中，所有广播的应用场景将会被IPv6组播所取代。

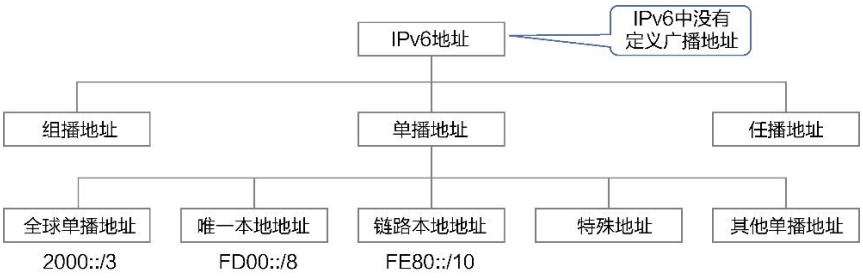


图11-8　IPv6地址分类

11.2.3　单播地址

1. 单播地址的组成

单播地址是点对点通信时使用的地址，此地址仅标识一个接口，网络负责把对单播地址发送的数据包传送到该接口上。

一个IPv6单播地址可以分为如下两部分，如图11-9所示。

- 网络前缀（Network Prefix）：*n* bit，相当于IPv4地址中的网络ID。
- 接口标识（Interface Identify）：（128-*n*）bit，相当于IPv4地址中的计算机ID。

常见的IPv6单播地址有全球单播地址（Global Unicast Address，GUA）、唯一本地地址（Unique Local Address，ULA）、链路本地地址（Link-Local Address，LLA）等，要求网络前缀和接口标识必须为64bit。

2. 全球单播地址

全球单播地址也被称为可聚合全球单播地址。该类地址全球唯一，用于需要有Internet访问需求的计算机，相当于IPv4的公网地址。

通常GUA的网络部分长度为64bit，接口标识也为64bit，如图11-10所示。



图11-9　IPv6地址组成



图11-10　全球单播地址的结构

IPv6全球单播地址的分配方式如下：顶级地址聚集机构TLA（即大的ISP或地址管理机构）获得大块地址，负责给次级地址聚集机构NLA（中小规模ISP）分配地址，NLA给站点级地址聚集机构SLA（子网）和网络用户分配地址。

可以向运营商申请全球单播地址或者直接向所在地区的IPv6地址管理机构申请。

- 全局路由前缀（Global Routing Prefix）：由提供商指定给一个组织机构，一般至少为45bit。
- 子网ID（Subnet ID）：组织机构根据自身网络需求划分子网。

- 接口ID（Interface ID）：用来标识一个设备（的接口）。

3. 唯一本地地址

唯一本地地址是IPv6私网地址，只能在内网使用。该地址空间在IPv6公网中不可被路由，因此不能直接访问公网。如图11-11所示，唯一本地地址使用FC00::/7（二进制为1111 1100:0000 0000::17）地址块，目前仅使用了FD00::/8地址段，FC00::/8预留为以后扩展用。唯一本地地址虽然只在有限范围内有效，但也具有全球唯一的前缀（虽然随机方式产生，但是冲突概率很低）。

8 bit	40 bit	16 bit	64 bit
1111 1101	Global ID	子网ID	接口标识

图11-11　唯一本地地址

4. 链路本地地址

IPv6中有种地址类型叫作链路本地地址，该地址用于在同一子网中的IPv6计算机之间进行通信。自动配置、邻居发现以及没有路由器的链路上的结点都使用这类地址。链路本地地址的有效范围是本地链路，如图 11-12 所示，前缀为FE80::/10。任意需要将数据包发往单一链路上的设备，以及不希望数据包发往链路范围外的协议都可以使用链路本地地址。当配置一个单播IPv6地址的时候，接口上会自动配置一个链路本地地址。链路本地地址可以和可路由的IPv6地址共存。

10 bit	54 bit	16 bit	64 bit
1111 1101 10	0	子网ID	接口标识
	固定为0		

图11-12　链路本地地址范围FE80::/10

IPv6地址的接口标识为64bit，用于标识链路上的接口。接口标识有许多用途，最常见的用法就是附加在链路本地地址前缀后面，形成接口的链路本地地址；或者在无状态自动配置中，附加在获取的IPv6全球单播地址前缀后面构成接口的全球单播地址。

5. 单播地址接口标识生成方式

IPv6单播地址接口标识可以通过以下三种方式生成：

- 手动配置；
- 系统自动生成；
- 通过IEE EUI-64（64-bit Extended Unique Identifier）规范生成。

其中EUI-64规范最为常用，此规范将接口的MAC地址转换为IPv6接口标识。IEEEE EUI-64规范是在MAC地址中插入FF-FE，MAC地址的第7bit取反，形成IPv64地址的64bit网络接口标识，如图11-13所示。

这种由MAC地址产生IPv6地址接口标识的方法可以减少配置的工作量，尤其是当采用无状态地址自动配置时，只需要获取一个IPv6前缀就可以与接口标识形成IPv6地址。

使用这种方式最大的缺点就是某些恶意者可以通过三层IPv6地址推算出二层MAC地址。



图11-13　EUI-64规范

11.2.4　组播地址

1. 组播地址的构成

与IPv4组播相同，IPv6组播地址标识多个接口，一般用于“一对多”的通信场景。IPv6组播地址只可以作为IPv6报文的目的地址。

组播地址就相当于广播电台的频道，某个广播电台在特定频道发送信号，收音机只要调到该频道，就能收到该广播电台的节目，没有调到该频道的收音机则忽略该信号。

如图 11-14 所示，组播源使用某个组播地址发送组播流，打算接收该组播信息的计算机需要加入该组播组，也就是网卡绑定该组播IP地址，并生成对应的组播MAC地址。加入该组播的所有接口接收组播数据包并对其进行处理，而没有绑定该组播地址的计算机则忽略组播信息。

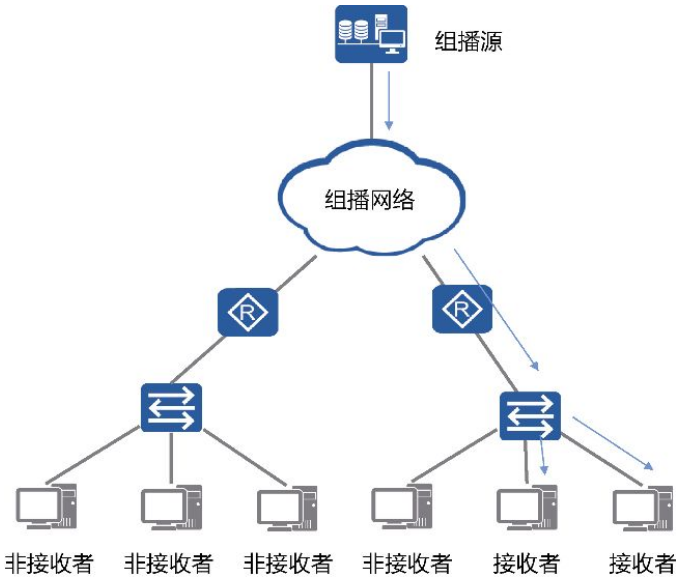


图11-14 组播示意图

组播地址以11111111（即FF）开头，如图11-15所示。

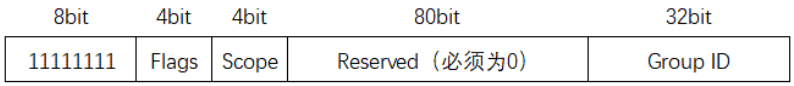


图11-15 组播地址的构成

Flags：用来表示永久或临时组播组。0000表示永久分配或众所周知。0001表示临时的。

Scope：表示组播的范围，如表11-2所示。

表11-2 组播范围

Scope取值	范　　围
0	表示预留

Scope取值	范　　围
1	表示节点本地范围，单个接口有效，仅用于Lookback通信
2	表示链路本地范围，例如FF02::1
5	表示站点本地范围
8	组织本地范围
E	表示全球范围
F	表示预留

Group ID：组播组ID。

Reserved：占80bit，必须为0。

2. 被请求节点组播地址

当一个节点具备了单播或任播地址，就会对应生成一个被请求节点组播地址，并且加入这个组播组。该地址主要用于邻居发现机制和地址重复检测功能。被请求节点组播地址的有效范围为本地链路范围。

如图11-16所示，被请求节点组播地址的前104位固定，前缀为：

FF02:0000:0000:0000:0000:0001:FF××：××××/104或缩写成FF02::1:FF××：××××/104。

将IPv6地址的后24位移下来填充到后面就形成被请求节点组播地址。

例如：IPv6地址2001::1234:5678/64的被请求节点组播地址为FF02::1:FF34:5678/104。

其中FF02::1:FF为固定部分，共104位。

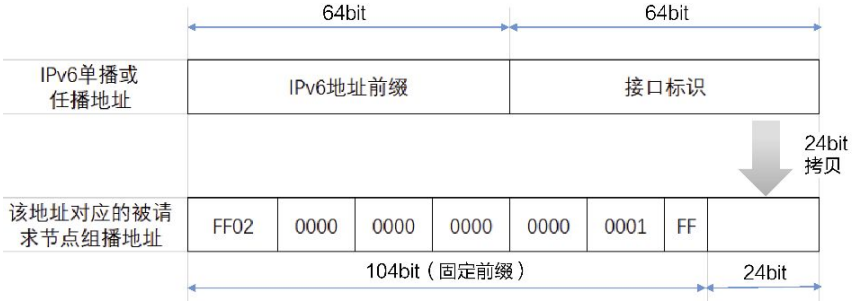


图11-16　被请求节点组播地址构成

在本地链路上，被请求节点的组播地址中只包含一个接口。只要知道一个接点的IPv6地址，就能计算出它的被请求节点的组播地址。

被请求节点组播地址的作用如下。

- 在IPv6中没有ARP。ICMP代替了ARP的功能，被请求节点的组播地址被节点用来获得相同本地链路上邻居节点的链路层地址。

- 用于重复地址检测（Duplicate Address Detection，DAD），在使用无状态自动配置将某个地址配置为自己的IPv6地址之前，节点利用DAD验证在其本地链路上该地址是否已经被使用。

由于只有目标节点才会侦听这个被请求节点组播地址，所以该组播报文可以被目标节点所接收，同时不会占用其他非目标节点的网络性能。

11.2.5　任播地址

任播地址标识一组接口，它与组播地址的区别在于发送数据包的方法。向任播地址发送的数据包并未被分发给组内的所有成员，而是发往该地址标识的“最近的”那个接口。

如图11-17所示，Web服务器1和Web服务器2分配了相同的IPv6地址2001:0DB8::84C2，该单播地址就成了任播地址。PC1和PC2需要访问Web服务，向2001:0DB8::84C2地址发送请求，PC1和PC2就会访问到距离它们最近（路由开销最小，也就是路径最短）的Web服务器。

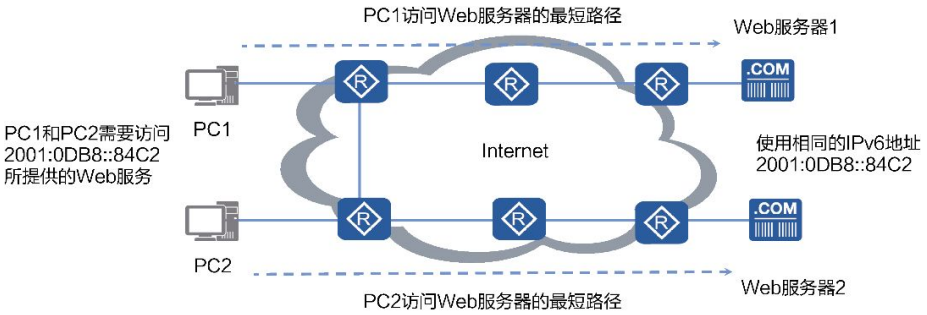


图11-17　任播地址的作用

任播过程涉及一个任播报文发起方和一个或多个响应方。

- 任播报文的发起方通常为请求某一服务（例如，Web服务）的主机。
- 任播地址与单播地址在格式上无任何差异，唯一的区别是一台设备可以给多个具有相同地址的设备发送报文。

在网络中运用任播地址有以下优势。

- 业务冗余。比如，用户可以通过多台使用相同地址的服务器来获取同一个服务（例如，Web服务）。这些服务器都是任播报文的响应方。如果不是采用任播地址通信，那么当其中一台服务器发生故障时，用户需要获取另一台服务器的地址才能重新建立通信。如果采用的是任播地址，当一台服务器发生故障时，任播报文的发起方能够自动与使用相同地址的另一台服务器通信，从而实现业务冗余。
- 提供更优质的服务。比如，某公司在A省和B省各部署了一台提供相同Web服务的服务器。基于路由优选规则，A省的用户在访问该公司提供的Web服务时，会优先访问部署在A省的服务器，提高访问速度，降低访问时延，这大大提升了用户体验。

任播地址从单播地址空间中分配，可使用单播地址的任何格式。因而，从语法上，任播地址与单播地址没有区别。当一个单播地址被分配给多于一个的接口时，它就将会转换为任播地址。被分配具有任播地址的节点必须得到明确的配置，从而知道它是一个任播地址。

11.2.6　常见的IPv6地址类型和范围

表11-3中列出了IPv6常见的地址类型和地址范围。

表11-3　IPv6常见的地址类型和地址范围

地址范围	描述
2000::/3	全球单播地址
2001:0DB8::/32	保留地址
FE80::/10	链路本地地址
FF00:;/8	组播地址
::/128	未指定地址
::1/128	环回地址

目前，有一小部分全球单播地址已经由IANA（Internet名称与数字地址分配机构ICANN的一个分支）分配给了用户。单播地址的格式是2000::/3，代表公共IP网络上任意可到达的地址。IANA负责将该段地址范围内的地址分配给多个区域Internet注册管理机构（RIR），RIR负责全球5个区域的地址分配。以下几个地址范围已经分配：2400::/12（APNIC）、2600::/12（ARIN）、2800::/12（LACNIC）、

2A00::/12（RIPE）和2C00::/12 （AFRINIC)，它们使用单一地址前缀来标识特定区域中的所有地址。

2000::/3地址范围还为文档示例预留了地址空间，例如2001:0DB8::/32。

链路本地地址只能在同一网段的节点之间通信使用。以链路本地地址为源地址或目的地址的IPv6报文不会被路由器转发到其他链路。链路本地地址的前缀是FE80::/10。使用IPv6通信的计算机会同时拥有链路本地地址和全球单播地址。

组播地址的前缀是FF00::/8。组播地址范围内的大部分地址是为特定组播组保留的。跟IPv4一样，IPv6组播地址还支持路由协议。IPv6中没有广播地址，用组播地址替代广播地址可以确保报文只发送给特定的组播组而不是IPv6网络中的任意终端。

0:0:0:0:0:0:0:0/128等于::/128。这是IPv4中0.0.0.0的等价地址，代表IPv6未指定地址。

0:0:0:0:0:0:0:1等于::1。这是IPv4中127.0.0.1的等价地址，代表本地环回地址。

11.3　IPv6地址配置

11.3.1　计算机和路由器的IPv6地址

配置了或启用了IPv6地址的计算机和路由器接口，会自动加入组播特定的组播地址，如图11-18所示。

所有节点的组播地址：FF02::1。

所有路由器的组播地址：FF02::2。

被请求节点组播地址：FF02:0:0:0:0:1:FFXX:XXXX。

所有OSPF路由器组播地址：FF02::5。

所有OSPF的DR路由器组播地址：FF02::6。

所有RIP路由器组播地址：FF02:0:0:0:0:0:0:9。

可以看到图11-18，计算机和路由器的接口都生成了两个“被请求节点组播地址”，分别由接口的链路本地地址和管理员分配的全球单播地址生成。

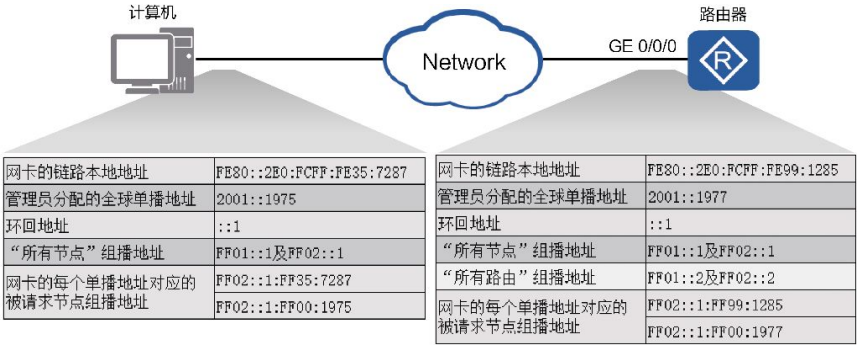


图11-18　IPv6接口地址和加入的特定的组播组

11.3.2　IPv6单播地址业务流程

计算机或路由器在发送IPv6报文之前要经历地址配置、重复地址检测、地址解析三个阶段（转发之前的3个阶段），如图11-19所示。在此过程中，邻居发现协议（Neighbor Discovery Protocol，NDP）扮演了重要角色，无状态自动配置、有状态地址配置、重复地址检测和地址解析都会用到NDP。

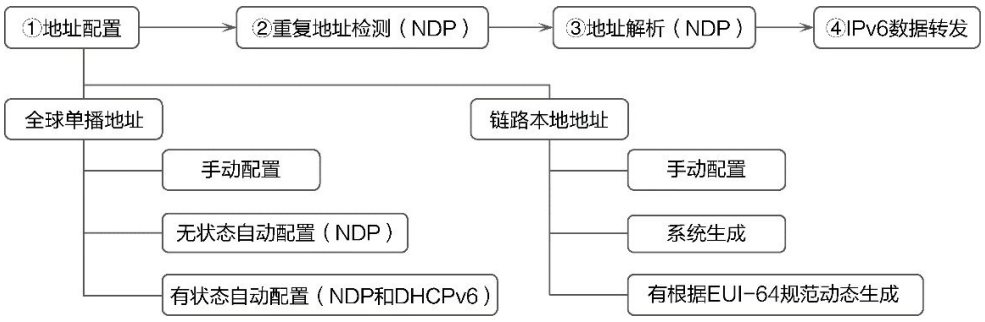


图11-19　接口配置IPv6地址的过程

IPv6地址配置到转发需要经历的过程如下。

- 全球单播地址和链路本地地址是接口上最常见的IPv6单播地址，一个接口可以配置多个IPv6地址。全球单播地址配置可以是手动

配置静态IPv6地址，可以是无状态自动配置，可以是有状态自动配置。链路本地地址通常是系统生成或根据EUI-64规范动态生成，很少手动配置。

- 重复地址检测（DAD）类似于IPv4中的免费ARP检测，用于检测当前地址是否与其他接口IPv6地址冲突。
- 地址解析类似于IPv4中的ARP请求，通过ICMPv6报文形成IPv6地址与数据链路层地址（一般是MAC地址）的映射关系。

μ　　IPv6配置完毕后，可以使用该地址转发IPv6数据。

11.3.3　邻居发现协议

邻居发现协议（NDP）作为IPv6的基础性协议，提供了地址自动配置、重复地址检测（DAD）、地址解析等功能，如图11-20所示。

- 无状态自动配置是IPv6的一个亮点功能，它使得IPv6计算机能够非常便捷地接入IPv6网络中，即插即用，无须手动配置烦冗的IPv6地址，无须部署应用服务器（例如DHCP服务器）为计算机分发地址。无状态自动配置机制使用了ICMPv6中的路由器请求（Router Solicitation，RS）报文以及路由器通告（Router Advertisement，RA）报文。通过无状态自动配置机制，链路上的节点可以自动获得IPv6全球单播地址。
- 重复地址检测使用ICMPv6 NS和ICMPv6 NA报文确保网络中无两个相同的单播地址。所有接口在使用单播地址前都需要做DAD。
- 地址解析是一种确定目的节点的链路层地址的方法。NDP中的地址解析功能不仅替代了原IPv4中的ARP，同时还用邻居不可达检测方法来维持邻居节点之间的可达性状态信息。地址解析过程使用两种ICMPv6报文：邻居请求（Neighbor Solicitation，NS）和邻居

通告（Neighbor Advertisement，NA）。这里的邻居是指附着在相同链路上的全部节点。

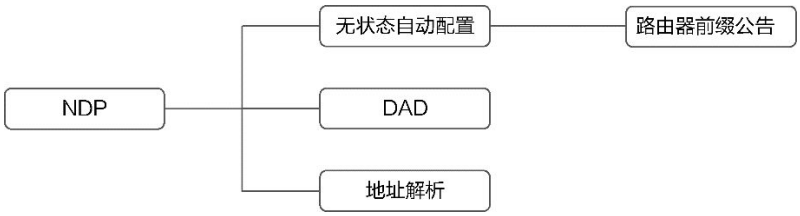


图11-20　NDP的功能

NDP使用ICMPv6报文，NDP封装在ICMPv6中，并使用类型字段标识NDP的不同报文。表11-4列出了NDP各种报文使用的类型字段。

表11-4　DNP使用的ICMPv6报文

ICMPv6类型	报文名称
133	路由器请求（RS）
134	路由器通告（RA）
135	邻居请求（NS）
136	邻居通告（NA）

表11-5列出了地址解析、前缀公告和DAD用到的报文类型。地址解析会用到NS135和NA136类型的报文，前缀公告会用到RS133和RA134类型的报文，DAD会用到NS135和NA136类型的报文。

表11-5　用到的报文类型

机　　制	RS133	RA134	NS135	NA136
地址解析			√	√
前缀公告	√	√		
DAD			√	√

11.3.4　IPv6地址配置方式

使用IPv6通信的计算机，可以人工指定静态地址，也可以设置成自动获取IPv6地址，如图11-21所示。自动配置有两种方式，即无状态自动配置和有状态自动配置。

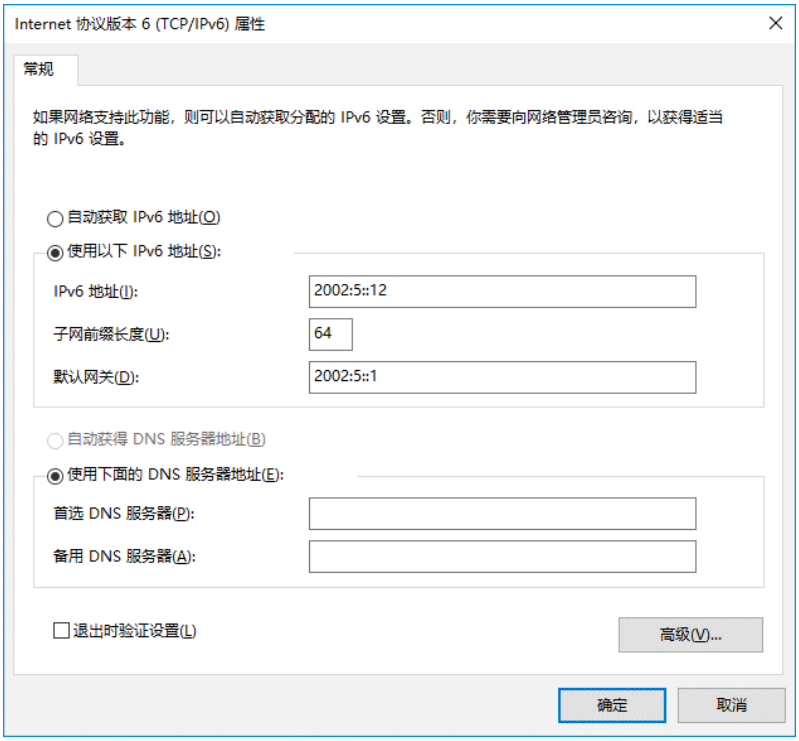


图11-21　IPv6静态地址和自动获取IPv6地址

11.3.5　IPv6地址自动配置的两种方式

IPv6支持地址分为有状态（Stateful）和无状态（Stateless）两种自动配置方式，路由器接口通告的RA报文中的M标记位和O标记位用于控制终端自动获取地址的方式。

M字段为管理地址配置标识（Managed Address Configuration Flag）。当M=0时，标识为无状态地址分配，客户端通过无状态协议（如ND）获得IPv6地址。当M=1时，标识为有状态地址分配，客户端通过有状态协议（如DHCPv6）获得IPv6地址。

O字段为其他有状态配置标识（Other stateful Configuration Flag）。当O=0时，标识客户端通过无状态协议（如ND）获取地址外的其他配置信息。当O=1时，标识客户端通过有状态协议（如DHCPv6）获取除地址外的其他配置信息，如DNS，SIP服务器等信息。

协议规定，若M=1，且O=1，才有意义。若M=0，O=1，无意义。

下面是无状态地址自动配置过程，RA中的M=0，O=0。

NDP的无状态自动配置包含两个阶段，链路本地地址的配置和全球单播地址的配置。当一个接口启用时，计算机会首先根据本地前缀FE80::/64和EUI-64接口标识符，为该接口生成一个链路本地地址。如果在后续的DAD中发生地址冲突，则必须对该接口手动配置本地链路地址，否则该接口将不可用。

接下来就以图11-22中计算机PC1的IPv6无状态自动配置为例，讲解IPv6无状态自动配置步骤。

- 计算机节点PC1在配置好链路本地地址后，发送RS报文，请求路由前缀信息。
- 路由器收到RS报文后，发送单播RA报文，携带用于无状态地址自动配置的前缀信息。M标记位为0，O标记位为0，同时路由器也会周期性地发送组播RA报文。
- PC1收到RA报文后，根据路由前缀信息和配置信息生成一个临时的全球单播地址。同时启动DAD，发送NS报文验证临时地址的唯一性，此时该地址处于临时状态。

- 链路上的其他节点收到DAD的NS报文后，如果没有节点使用该地址，则丢弃报文，否则产生应答NS的NA报文。
- PC1如果没有收到DAD的NA报文，说明地址是全局唯一的，则用该临时地址初始化接口，此时地址进入有效状态。

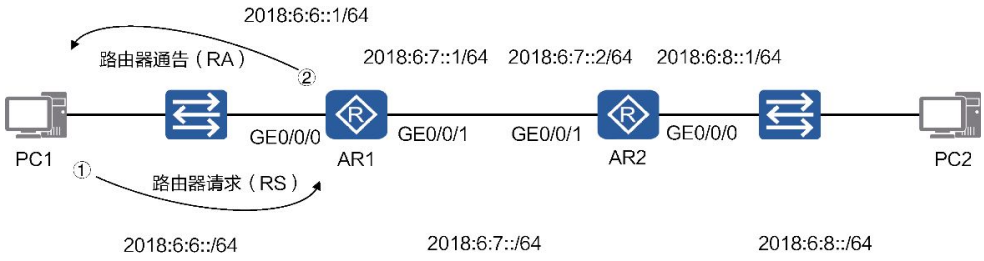


图11-22　IPv6无状态自动配置示意图

无状态地址配置的关键在于路由器完全不关心计算机的状态如何，比如是否在线等，因此称为无状态。无状态地址配置多用于物联网等终端，且终端不需要地址外的其他参数的场景。

接下来就以图11-23中计算机PC1的IPv6有状态自动配置（DHCPv6）为例，讲解IPv6有状态自动配置的步骤。

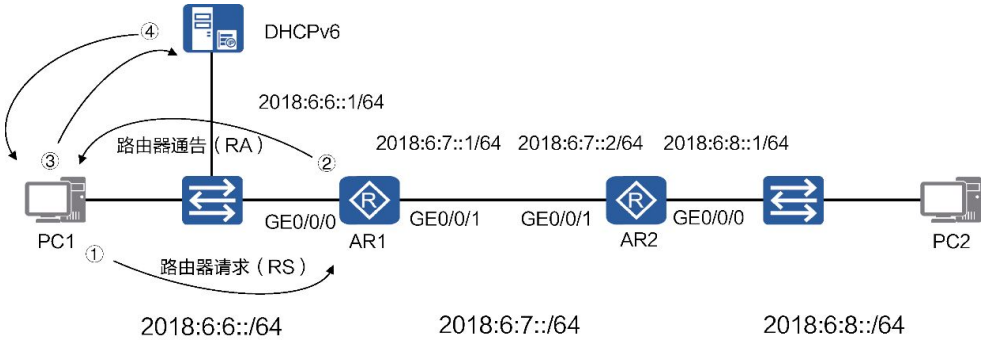


图11-23　有状态自动配置示意图

- PC1发送路由器请求（RS）。

- AR1路由器发送路由器通告（RA），RA报文中有两个标志位。M标记位是1，告诉PC1从DHCPv6服务器获取完整的128bit IPv6地址。O标记位是1，告诉PC1从DHCPv6服务器获取DNS等其他配置。如果这两个标记位都是0，则是无状态自动配置，不需要DHCPv6服务器。
- PC1发送DHCPv6征求消息。征求消息实际上就是组播消息，目标地址为FF02::1:2，是所有DHCPv6服务器和中继代理的组播地址。
- DHCPv6服务器给PC1提供IPv6地址和其他设置。此外，DHCPv6服务器端将会记录该地址的分配情况（这也是为什么被称为有状态）。

有状态地址配置要求网络中配置DHCPv6服务器，多用于公司内部有线终端的地址配置，便于地址进行管理。

11.4　实现IPv6地址自动配置

11.4.1　实现IPv6地址无状态自动配置

实验环境如图11-24所示，有3个IPv6网络，需要参照拓扑中标注的地址配置AR1和AR2路由器接口的IPv6地址。将Windows 10的IPv6地址设置成自动获取IPv6地址，以实现无状态自动配置。

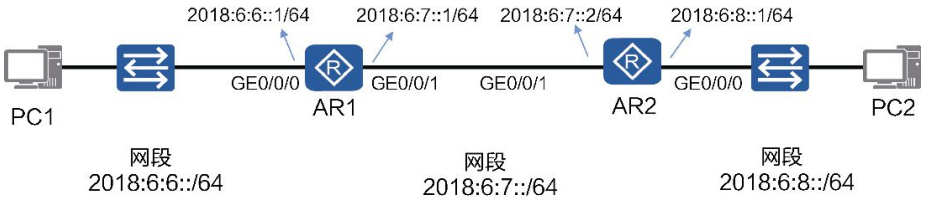


图11-24　IPv6地址无状态自动配置的实验拓扑

AR1路由器上的配置如下。

```
[AR1]ipv6                                                    --全局开启对IPv6的支持
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ipv6 enable                        --在接口上启用IPv6支持
[AR1-GigabitEthernet0/0/0]ipv6 address 2018:6:6::1 64   --添加IPv6地址
[AR1-GigabitEthernet0/0/0]ipv6 address auto link-local    --配置自动生成链路本地地址
[AR1-GigabitEthernet0/0/0]undo ipv6 nd ra halt --允许接口发送RA报文，默认不发送RA报文
[AR1-GigabitEthernet0/0/0]quit
[AR1]display ipv6 interface GigabitEthernet 0/0/0     --查看接口的IPv6地址
GigabitEthernet0/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE29:31F0
--链路本地地址
```

```
  Global unicast address(es):
   2018:6:6::1, subnet is 2018:6:6::/64          --全局单播地址
  Joined group address(es):                      --绑定的组播地址
   FF02::1:FF00:1
   FF02::2                                       --路由器接口绑定的组播地址
   FF02::1                                       --所有启用了IPv6的接口绑定的组播地址
   FF02::1:FF29:31F0                             --被请求节点组播地址
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1   --ND网络发现，地址冲突检测次数
  ……
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses  --计算机使用无状态自动配置
```

在Windows 10系统中，设置IPv6地址自动获得。打开命令提示符，输入ipconfig /all可以看到无状态自动配置生成的IPv6地址，同时也能看到链路本地地址（Windows系统称为本地连接IPv6地址）。IPv6网关是路由器的链路本地地址，如图11-25所示。

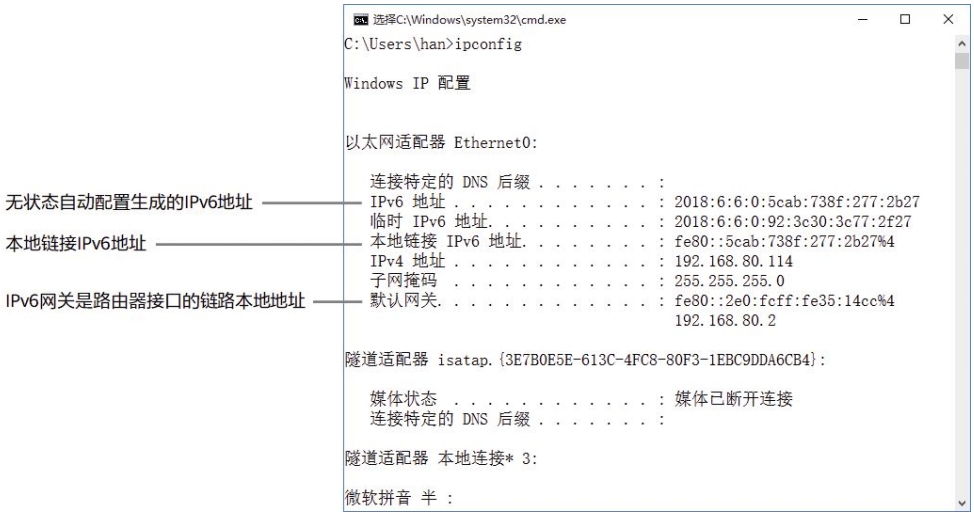


图11-25　无状态自动配置生成的IPv6地址

11.4.2　抓包分析RA和RS数据包

IPv6地址支持无状态地址自动配置，无须使用诸如DHCP之类的辅助协议，计算机即可获取IPv6前缀并自动生成接口ID。路由发现功能是IPv6地址自动配置功能的基础，主要通过RA、RS两种报文实现。

每台路由器为了让二层网络上的计算机和其他路由器知道自己的存在，定期以组播方式发送携带网络配置参数的RA报文。RA报文的Type字段值为134。

计算机接入网络后可以主动发送RS报文。RA报文是由路由器定期发送的，但是如果计算机希望能够尽快收到RA报文，它可以立刻主动发送RS报文给路由器。网络上的路由器收到RS报文后会立即向相应的计算机单播回应RA报文，告知计算机该网段的默认路由器和相关配置参数。RS报文的Type字段值为133。

为了让抓包工具能够捕获IPv6自动配置发送的RS报文和路由器响应的RA报文，先在Windows 10上运行抓包工具，然后在Windows 10上给IPv6指定一个静态IPv6地址，再选择“自动获取IPv6地址”，这样计算机就会发送RS报文，路由器发送RA报文进行响应。

如图11-26所示，在抓包工具捕获的数据包中，在显示筛选器输入icmpv6.type == 133，显示的第22个数据包是Windows 10发送的路由器请求（RS）数据包，使用的是ICMPv6协议，类型字段是133。可以看

到目标地址是组播地址ff02::2，代表网络中所有启用了IPv6的路由器接口，源地址是Windows 10的链路本地地址。

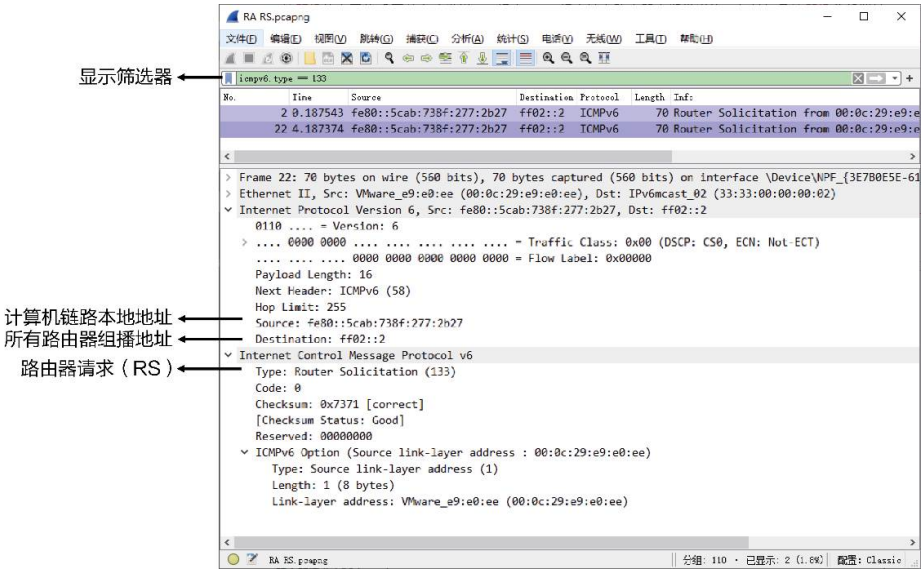


图11-26　RS数据包

如图11-27所示，在显示筛选器输入 icmpv6.type == 134，第60个数据包是路由器发送的路由器通告（RA）报文，目标地址是组播地址ff02::1（代表网络中所有启用了IPv6的接口），使用的是ICMPv6协议，类型字段是134。可以看到M标记位为0，O标记位为0，这就告诉Windows 10使用无状态自动配置，网络前缀为2018:6:6::。

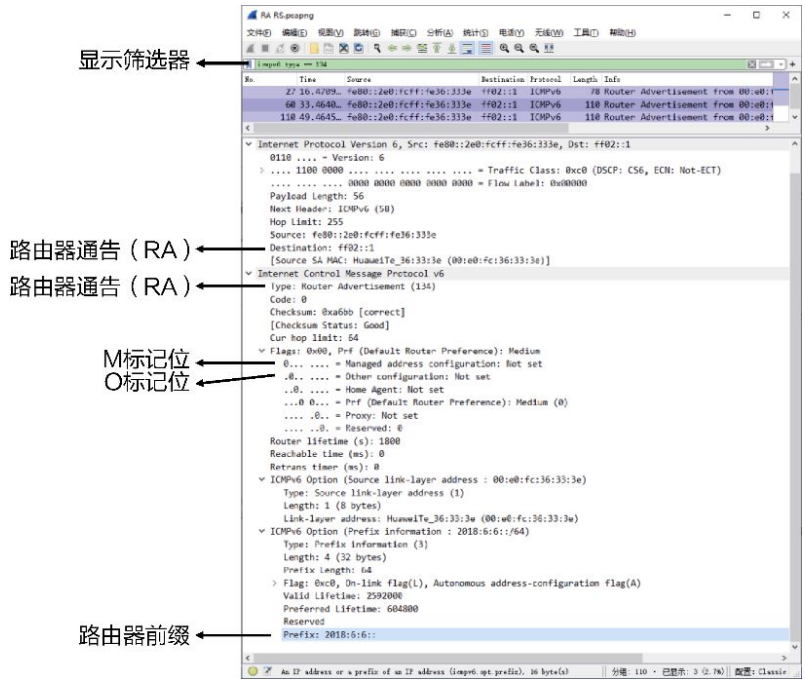


图11-27　路由器通告（RA）数据包

在Windows 10上查看IPv6的配置，如图11-28所示。打开命令提示符，输入netsh，输入interface ipv6，再输入show interface查看“Ethernet0”的索引，可以看到是4。再输入show interface “4”，可以看到IPv6相关的配置参数。“受管理的地址配置”是disabled，即不从DHCPv6服务器获取IPv6地址，“其他有状态的配置”是disabled，即不从DHCPv6服务器获取DNS等其他参数，也就是无状态自动配置。

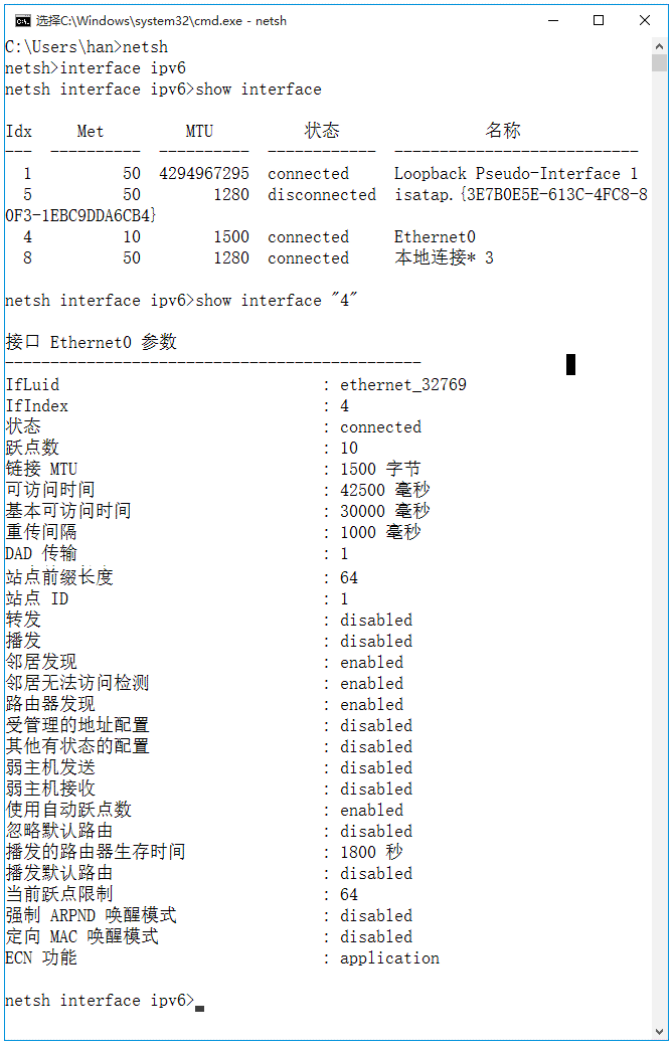


图11-28　查看IPv6的配置

11.4.3　实现IPv6地址有状态自动配置

使用DHCPv6可以为计算机分配IPv6地址和DNS等设置。

下面实现IPv6有状态地址自动配置，网络环境如图11-29所示。配置AR1路由器为DHCPv6服务器，配置GE 0/0/0接口，路由器通告报文中

的M标记位为1，O标记位也为1，Windows 10会从DHCPv6获取IPv6地址。



图11-29　有状态自动配置的网络拓扑

```
[AR1]ipv6                                          --启用IPv6
[AR1]dhcp enable                                   --启用DHCP功能
[AR1]dhcpv6 duid ?                                 --生成DHCP唯一标识的方法
  ll    DUID-LL
  llt   DUID-LLT
[AR1]dhcpv6 duid llt                               --使用llt方法生成DHCP唯一
标识
[AR1]display dhcpv6 duid                           --显示DHCP唯一标识
The device's DHCPv6 unique identifier:
0001000122AB384A00E0FC2931F0
[AR1]dhcpv6 pool localnet                          --创建IPv6地址池，名称为
localnet
[AR1-dhcpv6-pool-localnet]address prefix 2018:6:6::/64       --地址
前缀
[AR1-dhcpv6-pool-localnet]excluded-address 2018:6:6::1       --排除
的地址
[AR1-dhcpv6-pool-localnet]dns-domain-name huawei.com         --域名
后缀
[AR1-dhcpv6-pool-localnet]dns-server 2018:6:6::2000          --DNS
服务器
[AR1-dhcpv6-pool-localnet]quit
```

查看配置的DHCPv6地址池。

```
<AR1>display dhcpv6 pool
DHCPv6 pool: localnet
  Address prefix: 2018:6:6::/64
   Lifetime valid 172800 seconds, preferred 86400 seconds
   2 in use, 0 conflicts
  Excluded-address 2018:6:6::1
```

```
  1 excluded addresses
  Information refresh time: 86400
  DNS server address: 2018:6:6::2000
  Domain name: 91xueit.com
  Conflict-address expire-time: 172800
  Active normal clients: 2
```

配置AR1路由器的GE 0/0/0接口。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ipv6 enable
[AR1-GigabitEthernet0/0/0]dhcpv6 server localnet  --指定从localnet
地址池选择地址
[AR1-GigabitEthernet0/0/0]undo ipv6 nd ra halt    --允许发送RA报文
[AR1-GigabitEthernet0/0/0]ipv6 nd autoconfig managed-address-flag
--M标记位为1
[AR1-GigabitEthernet0/0/0]ipv6 nd autoconfig other-flag
--O标记位为1
[AR1-GigabitEthernet0/0/0]quit
```

为了让抓包工具能够捕获IPv6自动配置发送的RS报文和路由器响应的RA报文，先在Windows 10上运行抓包工具，然后在Windows 10上给IPv6指定一个静态IPv6地址，再选择“自动获取IPv6地址”，这样计算机就会发送RS报文，路由器就会发送RA报文进行响应。从抓包工具中找到路由器通告（RA）报文，如图11-30所示，可以看到M标记位和O标记位的值都为1。计算机也通告了路由器前缀，但计算机还是会从DHCPv6服务器获取IPv6地址和其他设置。

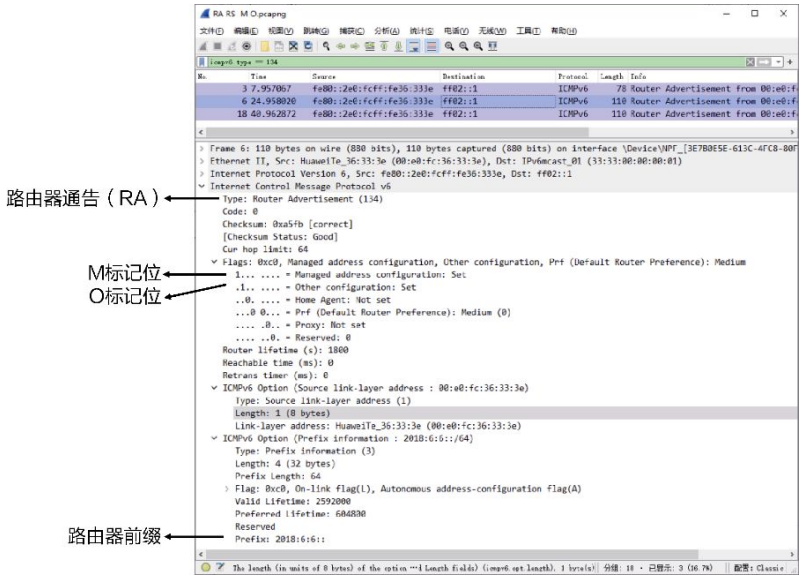


图11-30　捕获的RA数据包

在Windows 10中打开命令提示符，如图11-31所示，输入ipconfig /all可以看到从DHCPv6获得的IPv6配置，又可以看到从DHCPv6获得的“DNS后缀搜索列表”为“huawei.com”、DNS、租约时间。

```
C:\Windows\system32\cmd.exe
C:\Users\han>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : Windows10
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : huawei.com

以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . . . : huawei.com
   描述. . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Conne
ction
   物理地址. . . . . . . . . . . . . : 00-0C-29-E9-E0-EE
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2018:6:6::2(首选)
   获得租约的时间  . . . . . . . . . : 2020年4月1日 15:37:33
   租约过期的时间  . . . . . . . . . : 2020年4月3日 15:37:33
   IPv6 地址 . . . . . . . . . . . . : 2018:6:6:0:5cab:738f:277:2b27(首选)
   临时 IPv6 地址. . . . . . . . . . : 2018:6:6:0:29fa:20f4:59af:7df5(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::5cab:738f:277:2b27%4(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.80.114(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : fe80::2e0:fcff:fe35:14cc%4
                                       192.168.80.2
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-26-15-F4-DE-00-0C-29-E9-E
0-EE
   DNS 服务器  . . . . . . . . . . . : 2018:6:6::2000
```

图11-31　查看从DHCPv6获得的IPv6配置

如图11-32所示，输入show interface “4”，可以看到“受管理的地址配置”为enabled，“其他有状态的配置”为enabled。

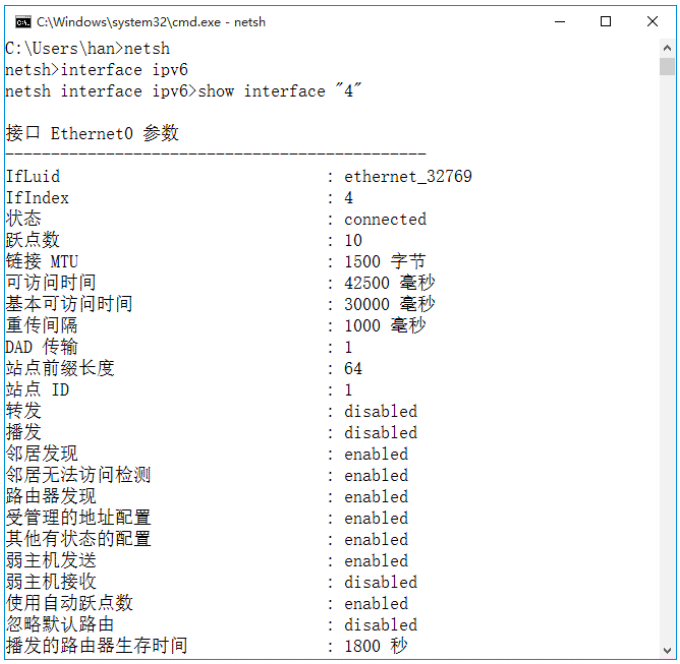


图11-32　IPv6的状态

11.5　IPv6路由

IPv6网络畅通的条件和IPv4的一样，数据包有去有回网络才能通。对于没有直连的网络，需要人工添加静态路由，或使用动态路由协议学习到各个网段的路由。

支持IPv6的动态路由协议也都需要新的版本。IPv6取消了广播地址，因此完全使用广播流量的任何协议都不会再用了。

在IPv6中仍然使用的路由协议都有了新的名字，支持IPv6的OSPF协议是OSPFv3（OSPF第3版），支持IPv4的OSPF协议是OSPFv2 （OSPF第2版）。

接下来将会演示配置IPv6的静态路由，以及配置支持IPv6的动态路由协议OSPFv3。

11.5.1　IPv6静态路由

如图11-33所示，网络中有3个IPv6网段、两个路由器，参照图中标注的地址配置路由器接口的IPv6地址。在AR1和AR2上添加静态路由，使得这3个网络能够相互通信。



图11-33　静态路由的网络拓扑

在AR1上启用IPv6，配置接口启用IPv6，配置接口的IPv6地址，添加到2018:6:8::/64网段的路由。

```
[AR1]ipv6
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ipv6 enable
[AR1-GigabitEthernet0/0/0]ipv6 address 2018:6:6::1 64
[AR1-GigabitEthernet0/0/0]ipv6 address auto link-local
[AR1-GigabitEthernet0/0/0]undo ipv6 nd ra halt
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]ipv6 enable
[AR1-GigabitEthernet0/0/1]ipv6 address 2018:6:7::1 64
[AR1-GigabitEthernet0/0/1]quit
```

添加到2018:6:8::/64网段的静态路由。

```
[AR1]ipv6 route-static 2018:6:8:: 64 2018:6:7::2
```

显示IPv6静态路由。

```
[AR1]display ipv6 routing-table protocol static
Public Routing Table : Static
Summary Count : 1
Static Routing Table's Status : < Active >
Summary Count : 1
 Destination  : 2018:6:8::                      PrefixLength : 64
 NextHop      : 2018:6:7::2                     Preference   : 60
 Cost         : 0                               Protocol     :
Static
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1            Flags        : RD

Static Routing Table's Status : < Inactive >
Summary Count : 0
```

显示IPv6路由表。

```
[AR1]display ipv6 routing-table
```

配置AR2路由器启用IPv6，在接口上启用IPv6，配置接口的IPv6地址，添加到2018:6:6::/64网段的静态路由。

```
[AR2]ipv6
[AR2]interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1]ipv6 enable
[AR2-GigabitEthernet0/0/1]ipv6 address 2018:6:7::2 64
[AR2-GigabitEthernet0/0/1]quit
[AR2]interface GigabitEthernet 0/0/0
[AR2-GigabitEthernet0/0/0]ipv6 enable
[AR2-GigabitEthernet0/0/0]ipv6 address 2018:6:8::1 64
[AR2-GigabitEthernet0/0/0]quit
[AR2]ipv6 route-static 2018:6:6:: 64 2018:6:7::1
```

在AR1上测试到2018:6:8::1是否畅通。

```
<AR1>ping ipv6 2018:6:8::1
 PING 2018:6:8::1 : 56  data bytes, press CTRL_C to break
  Reply from 2018:6:8::1 bytes=56 Sequence=4 hop limit=64  time =
20 ms
  Reply from 2018:6:8::1 bytes=56 Sequence=5 hop limit=64  time =
20 ms
  Reply from 2018:6:8::1 bytes=56 Sequence=5 hop limit=64  time =
20 ms
  Reply from 2018:6:8::1 bytes=56 Sequence=4 hop limit=64  time =
20 ms
  Reply from 2018:6:8::1 bytes=56 Sequence=5 hop limit=64  time =
20 ms

 --- 2018:6:8::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/32/80 ms
```

删除IPv6静态路由。

```
[AR1]undo ipv6 route-static 2018:6:8:: 64
[AR2]undo ipv6 route-static 2018:6:6:: 64
```

11.5.2　OSPFv3

新版本的OSPF与IPv4中的OSPF有许多相似之处。

OSPFv3和OSPFv2的基本概念是一样的，它仍然是链路状态路由协议，它将整个网络或自治系统分成不同区域，从而使网络层次分明。

在OSPFv2中，路由器ID（RID）由分配给路由器的最大IP地址决定（也可以由你来分配）。在OSPFv3中，可以分配RID、地区ID和链路状态ID，链路状态ID仍然是32位的值，但却不能再使用IP地址找到了，因为IPv6的地址为128位。根据这些值的不同分配，配置会有相应的改动。从OSPF包的报头中还删除了IP地址信息，这使得新版本的OSPF几乎能通过任何网络层协议来进行路由。

在OSPFv3中，邻接和下一跳属性使用链路本地地址，但仍然使用组播流量来发送更新和应答信息。对于OSPF路由器，地址为FF02::5；对于OSPF指定路由器，地址为FF02::6，这些新地址分别用来替换224.0.0.5和224.0.0.6。

下面就展示配置OSPFv3的过程。如图11-34所示，网络中的路由器接口地址已经配置完成，现在需要在路由器AR1和AR2上配置OSPFv3。

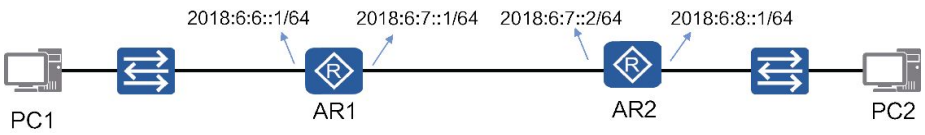


图11-34　配置OSPFv3

AR1上的配置如下。

```
[AR1]ospfv3 1                                          --启用OSPFv3，指定进
程号
[AR1-ospfv3-1]router-id 1.1.1.1                        --指定router-id，必须
唯一
[AR1-ospfv3-1]quit
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ospfv3 1 area 0              --在接口上启用
OSPFv3，指定区域编号
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]ospfv3 1 area 0
[AR1-GigabitEthernet0/0/1]quit
```

AR2上的配置如下。

```
[AR2]ospfv3 1                                          --启用OSPFv3，指定进
程号
[AR2-ospfv3-1]router-id 1.1.1.2
[AR2-ospfv3-1]quit
[AR2]interface GigabitEthernet 0/0/0
[AR2-GigabitEthernet0/0/0]ospfv3 1 area 0
[AR2-GigabitEthernet0/0/0]quit
[AR2]interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1]ospfv3 1 area 0
[AR2-GigabitEthernet0/0/1]quit
```

查看OSPFv3学习到的路由。

```
[AR1]display ipv6 routing-table protocol ospfv3
Public Routing Table : OSPFv3
Summary Count : 3
OSPFv3 Routing Table's Status : < Active >
Summary Count : 1
 Destination  : 2018:6:8::                          PrefixLength : 64
 NextHop      : FE80::2E0:FCFF:FE1E:7774            Preference   : 10
 Cost         : 2                                   Protocol     :
OSPFv3
 RelayNextHop : ::                                  TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1                Flags        : D
……
```

11.6　习题

1．关于IPv6地址2031:0000:72C:0000:0000:09E0:839A:130B，下列哪些缩写是正确的？（　　）（选择两个答案）

A．2031:0:720C:0:0:9E0:839A:130B

B．2031:0:720C:0:0:9E:839A:130B

C．2031::720C::9E:839A:130B

D．2031:0:720C::9E0:839A:130B

2．下列哪些IPv6地址可以被手动配置在路由器接口上？（　　）（选择两个答案）

A．fe80:13dc::1/64

B．ff00:8a3c::9b/64

C．::1/128

D．2001:12e3:1b02::21/64

3．关于IPv6的描述正确的是（　　）。（选择两个答案）

A．IPv6的地址长度为64位

B. IPv6的地址长度为128位

C. IPv6地址有状态配置使用DHCP服务器分配地址和其他设置

D. IPv6地址无状态配置使用DHCPv6服务器分配地址和其他设置

4. IPv6地址不包括下列哪种类型的地址？（　　）

A. 单播地址

B. 组播地址

C. 广播地址

D. 任播地址

5. 下列选项中，哪个是链路本地地址的地址前缀？（　　）

A. 2001::/10

B. FE80::/10

C. FEC0::/10

D. 2002::/10

6. 下面哪条命令是添加IPv6默认路由的命令？（　　）

A. [AR1]ipv6 route-static :: 0 2018:6:7::2

B. [AR1]ipv6 route-static ::1 0 2018:6:7::2

C. [AR1]ipv6 route-static :: 64 2018:6:7::2

D. [AR1]ipv6 route-static :: 128 2018:6:7::2

7. IPv6网络层协议有哪些？（　　）

A. ICMPv6、IPv6、ARP、ND

B. ICMPv6、IPv6、MLD、ND

C. ICMPv6、IPv6、ARP、IGMPv6

D. ICMPv6、IPv6、MLD、ARP

8. 在VRP系统中配置DHCPv6，下列哪些形式的DUID可以被配置？（　　）

A. DUID-LL　　B. DUID-LLT

C. DUID-EN　　D. DUID-LLC

9. 全球单播地址由以下哪些部分组成？（　　）（多选）

A. Protocol ID

B. Interface ID

C. Subnet ID

D. Global Routing Prefix

10. IPv6无状态自动配置使用的RA报文在以下哪种报文类型中承载？（　　）

A. IGMPv6

B. ICMPv6

C. UPv6

D. TCPv6

11. 链路本地单播地址的接口标识总长度为多少bit？（　　）

A. 48bit

B. 32bit

C. 64bit

D. 96bit

12. IPv6地址FE80::2EO:FCFF:FE6F:4F36属于哪一类？（　　）

A. 组播地址

B. 任播地址

C. 链路本地地址

D．全球单播地址

13．DHCPv6客户端在向DHCPv6服务器发送请求报文之前，会发送以下哪个报文？（　　）

A．RA

B．RS

C．NA

D．NS

第12章　广域网

本章内容

- 广域网
- PPP介绍
- 配置PPP
- PPPoE

本章讲解广域网链路使用的协议。点到点链路可以使用HDCL、PPP等数据链路层协议。数据包经过不同的数据链路时要封装成该数据链路层协议的帧格式。

点对点协议（Point-to-Point Protocol，PPP）为在点对点链路上传输多协议的数据包提供了一个标准方法。本章展示配置PPP的身份验证和地址协商功能，同时抓包分析PPP的帧格式。

以太网协议不支持接入设备的身份验证功能。PPP支持接入身份验证，并且为远程计算机分配IP地址。如果让以太网接入也具有验证用户身份，以及验证通过之后再分配上网地址的功能，那就需要用到PPPoE（PPP over Ethernet）。本章展示如何配置路由器为PPPoE服务器，Windows操作系统作为PPPoE客户端通过拨号访问Internet，还列出了将路由器配置为PPPoE客户端以实现通过PPPoE拨号上网的配置步骤。

12.1　广域网

广域网（Wide Area Network，WAN）通常跨接很大的物理范围，覆盖的范围从几十千米到几千千米不等，它能连接多个城市或国家，或横跨几个大洲来提供远距离通信，从而形成国际性的远程网络。局域网通常作为广域网的终端用户与广域网相连。如图12-1所示，一家公司在北京、上海和深圳各有一个局域网，它们通过电信运营商的网络互连，电信运营商为企业提供广域网连接。

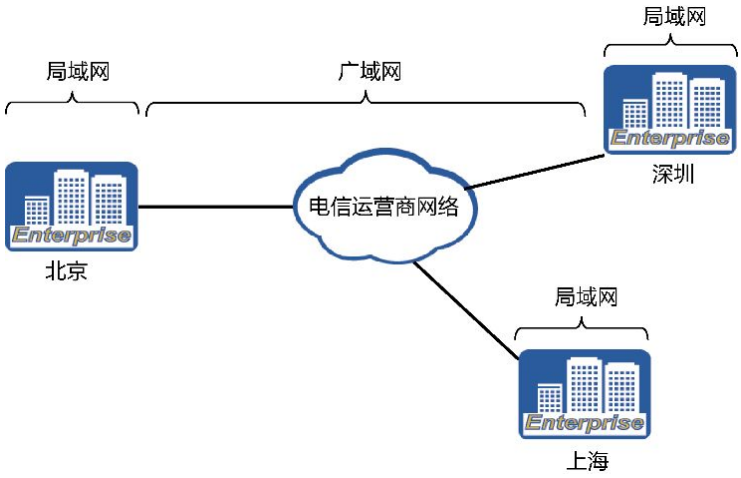


图12-1　局域网和广域网示意图

局域网通常由企业购买路由器、交换机，自己组建和维护。广域网一般由电信部门或公司负责组建、管理和维护，并向全社会提供面向通信的有偿服务。家庭用户通过ADSL上网或通过光纤接入Internet，这就是广域网。

如图12-2所示，局域网1和局域网2通过广域网线路连接。图12-2中路由器连接广域网的接口为Serial接口，即串行接口。Serial接口

有多个标准，图中展示了“同异步WAN接口”和“非通道化E1/T1 WAN接口”两种接口。

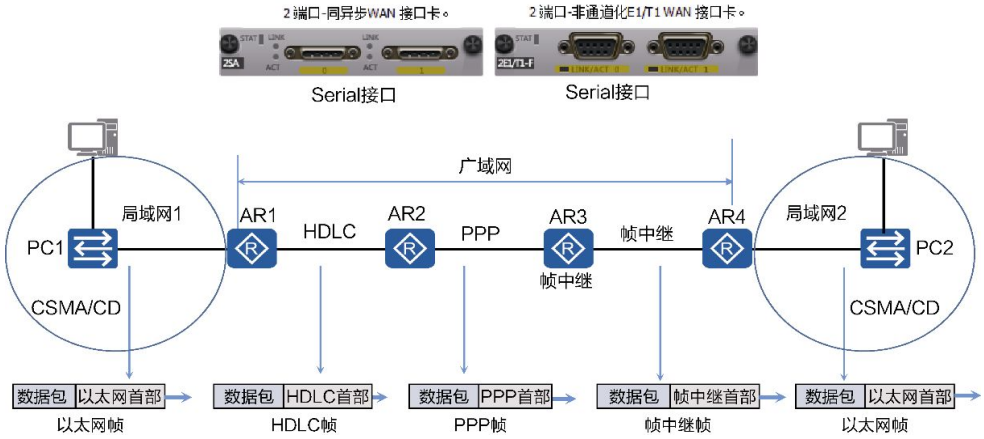


图12-2　广域网示意图

广域网链路可以有不同的协议，如图12-2所示。AR1路由器和AR2路由器之间的串行链路使用的是HDLC协议，AR2和AR3之间的串行链路使用的是PPP，AR3和AR4之间使用帧中继交换机连接，它们使用Frame Relay协议。

不同的链路使用不同的数据链路层协议，每种数据链路层协议都定义了相应的数据链路层封装（首部）。数据包经过不同的链路，就要封装成不同的帧。图12-2展示了PC1给PC2发送数据包的过程，首先经过以太网，要把数据包封装成以太网帧，在AR1和AR2之间的链路上要把数据包封装成HDLC帧，在AR2和AR3之间的链路上要把数据包封装成PPP帧，在AR3和AR4之间的链路上要把数据包封装成帧中继帧，从AR4发送到PC2要将数据包封装成以太网帧。

本章重点讲解PPP和PPPoE两种协议，并能过抓包来查看不同的PPP的帧格式。

12.2 PPP介绍

PPP是Point-to-Point Protocol的简称，中文翻译为点对点协议。PPP为在点对点连接上传输多协议数据包提供了一个标准方法。与以太网协议一样，PPP也是一个数据链路层协议。以太网协议定义了以太帧的格式，PPP也定义了自己的帧格式，这种格式的帧称为PPP帧。

PPP的前身是SLIP（Serial Line Internet Protocol）和CSLIP（Compressed SLIP），这两种协议现在已基本不再使用。但PPP自20世纪90年代推出以来，一直得到了广泛的应用。

PPP现在已经成为使用最广泛的Internet接入的数据链路层协议之一。PPP可以和ADSL、Cable Modem、LAN等技术结合起来完成各类型的宽带接入。家庭中使用最多的宽带接入方式就是PPPoE（PPP over Ethernet）。这是一种利用以太网（Ethernet）资源，在以太网上运行PPP来对用户进行接入认证的技术，PPP负责在用户端和运营商的接入服务器之间建立通信链路。

以太网协议工作在以太网接口和以太网链路上，而PPP工作在串行接口和串行链路上。串行接口本身的种类是多种多样的，如EIA RS-232-C接口、EIARS-422接口、EIARS-423接口、ITU-T V.35接口等，这些都是一些常见的串行接口，并且都支持PPP。事实上，任何串行接口，只要支持全双工通信方式，便是可以支持PPP的。另外，PPP对于串行接口的信息传输速率没有什么特别的规定，只要求串行链路两端

的串行接口在速率上保持一致即可。在本章中，我们把支持并运行PPP的串行接口统称为PPP接口。

12.2.1 PPP原理

PPP的封装方式在很大程度上参照了HDLC协议的规范，如图12-3所示。PPP原原本本地使用了HDLC协议封装中的标记字段和FCS校验码字段。此外，鉴于PPP纯粹是一种应用于点到点环境中的协议，任何一方发送的消息都只会由固定的另一方接收并处理，地址字段存在的意义已经不大，因此PPP地址字段的取值以全1的方式被明确下来，表示这条链路上的所有接口。最后，PPP控制字段的取值也被明确为0x03。

PPP明确了数据帧中很多字段的取值：PPP的数据帧封装格式如图12-3所示。首部有5字节，其中F字段为帧开始定界符（0x7e），占1字节；A字段为地址字段，占1字节；C字段为控制字段，占1字节，协议字段用来标明信息部分是什么协议，占2字节。尾部有3字节，其中2字节是帧校验序列，1字节是帧结束定界符（0x7e）。信息部分不超过1500字节。

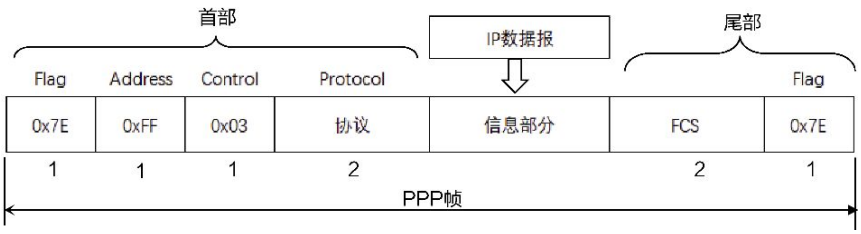


图12-3　PPP的封装格式

PPP的封装也与HDLC协议有一点区别，那就是PPP在封装字段中添加了协议字段。这个协议字段是为了标识这个数据帧的消息负载是使用的什么协议进行封装的。

PPP是一种分层的协议，如图12-4所示，它由3个部分组成，LCP和NCP可以认为是PPP协议的工作过程，链路控制的帧和网络控制的帧都封装在PPP帧中。

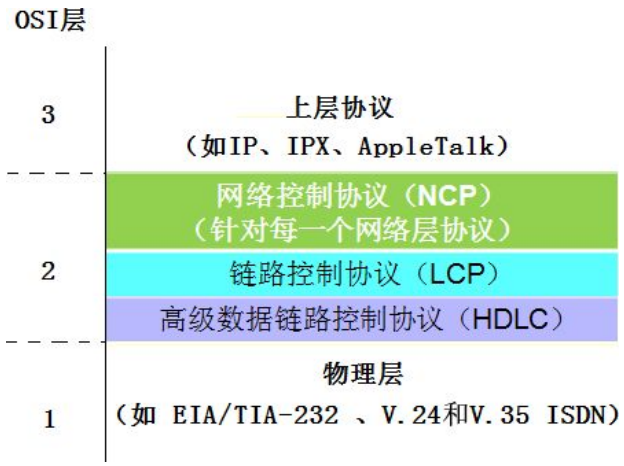


图12-4 PPP分层

为了能够适应更加广泛的物理介质和网络层传输协议，PPP采用了分层的体系结构。这个体系架构的上层是网络控制协议（Network Control Protocol，NCP），NCP的作用是为网络层协议IPv4、IPv6、IPX、AppleTalk等协商和配置参数。NCP并不是一个特定的协议，而是PPP架构上层中一系列控制不同网络层传输协议的协议总称。不同的网络层协议都有一个对应的NCP，譬如IPv4协议对应的是IPCP，IPv6协议对应的是IPv6CP，IPX协议对应的是IPXCP，AppleTalk协议对应的是ATCP等。NCP下面是链路控制协议（Link Control Protocol，LCP），

链路控制协议的作用是发起、监控和终止连接，通过协商的方式对接口进行自动配置，执行身份认证等。

这些上下层关系体现在PPP连接的协商和建立阶段的层面，在两台设备要通过PPP在一条串行链路上传输数据之前，它们首先需要通过LCP来协商、建立数据链路，然后再通过NCP来协商网络层的配置。请读者不要因为这种上下层关系就误以为一个IPv4数据包会逐层封装IPCP头部和LCP头部。实际上，在上面所说的这两个阶段中，NCP消息和LCP都被封装在PPP数据帧中，然后再根据下层不同的物理介质对PPP数据帧执行成帧。

PPP工作过程如下。

（1）建立、配置及测试数据链路的链路控制协议（Link Control Protocol，LCP）。它允许通信双方进行协商，以确定不同的选项。这些选项包括最大接收单元、认证协议、协议字段压缩等。对于没有协商的参数，使用默认操作。

（2）认证协议。如果一端需要身份验证，就需要对方出示账户和密码进行身份验证。最常用的是密码验证协议PAP和挑战握手验证协议CHAP。PAP和CHAP通常被用在PPP封装的串行线路上，以提供安全性认证。

（3）LCP协商完参数和身份验证后，PPP就会开始通过上层协议对应的网络控制协议（Network Control Protocol，NCP）来协商上层协议的配置参数。NCP为网络层协商可选的配置参数。比如IPCP需要协商

的配置参数包括消息的PPP和IP头部是否压缩，使用什么算法进行压缩，以及PPP接口的IPv4地址。

PPP的特点如下。

- PPP既支持同步传输又支持异步传输，而X.25、FR（Frame Relay）等数据链路层协议仅支持同步传输，SLIP仅支持异步传输。
- PPP具有很好的扩展性，例如，当需要在以太网链路上承载PPP时，PPP可以扩展为PPPoE。
- PPP提供了LCP（Link Control Protocol）协议，LCP用于各种链路层参数的协商。
- PPP提供了各种NCP（Network Control Protocol），如IPCP、IPXCP，用于各网络层参数的协商，能更好地支持网络层协议。
- PPP提供了认证协议：CHAP（Challenge-Handshake Authentication Protocol）、PAP（Password Authentication Protocol），它们能更好地保证网络的安全性。
- 无重传机制，网络开销小，速度快。

12.2.2 PPP基本工作流程

PPP是一种点对点协议，它只涉及位于PPP链路两端的两个接口。当我们在分析和讨论其中一个接口时，习惯上就把这个接口叫作本地接口或本端接口，而把另一个接口叫作对端接口或远端接口。

通过串行链路连接起来的本地接口和对端接口在上电之后，并不能马上就开始相互发送携带诸如IP报文这样的网络层数据单元的PPP

帧。本地接口和对端接口在开始相互发送携带诸如IP报文这样的网络层数据单元的PPP帧之前，必须经过一系列复杂的协商过程（甚至还可能包括认证过程），这一过程也称为PPP的基本工作流程。

PPP基本工作流程总共包含了5阶段，分别是：链路关闭阶段（Link Dead阶段），链路建立阶段（Link Establishment阶段），认证阶段（Authentication阶段），网络层协议阶段（Network Layer Protocol阶段），链路终结阶段（Link Termination阶段）。

图12-5展示了PPP的链路协商阶段、认证阶段和网络层协议阶段（未标识）。

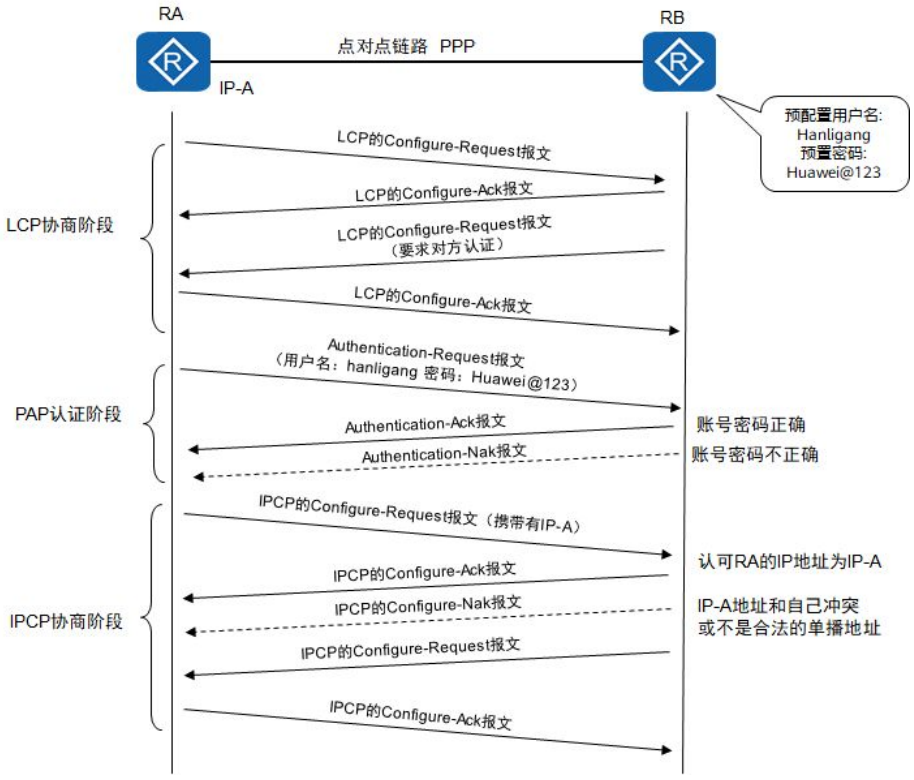


图12-5　PPP工作流程

PPP基本工作流程的第一个阶段是Link Dead阶段。在此阶段，PPP接口的物理层功能尚未进入正常状态。只有当本端接口和对端接口的物理层功能都进入正常状态之后，PPP才能进入下一个工作阶段，即Link Establishment阶段。

当本端接口和对端接口的物理层功能都进入正常状态之后，PPP便会自动进入Link Establishment阶段。在此阶段，本端接口会与对端接口相互发送携带LCP报文的PPP帧。简单来说，此阶段也就是双方交互LCP报文的阶段。通过LCP报文的交互，本端接口会与对端接口协商若干基本而重要的参数，以确保PPP链路可以正常工作。例如，本端接口会与对端接口对的MRU（Maximum Receive Unit）参数进行协商。所谓MRU，就是PPP帧中Information字段所允许的最大长度（字节数）。如果本端接口因为某种原因而要求所接收的PPP帧的Information字段的长度不得超过1800字节（即本端接口的MRU为1800），而对端接口却发送了Information字段为2000字节的PPP帧，那么，在这种情况下，本端接口就无法正确地接收和处理这个Information字段为2000字节的PPP帧，通信就会因此而产生故障。因此，为了避免这种情况的发生，本端接口和对端接口在Link Establishment阶段就必须对MRU这个参数进行协商并取得一致意见，此后，本端接口就不会发送Information字段超过对端MRU的PPP帧，对端接口也不会发送Information字段超过本端MRU的PPP帧。

在Link Establishment阶段，本端接口和对端接口还必须约定好是直接进入Network Layer Protocol阶段，还是先进入

Authentication阶段，再进入Network Layer Protocol阶段。如果需要进入Authentication阶段，还必须约定好使用什么样的认证协议来进行认证。PAP身份验证方式的账号和密码在网络中明文传输，CHAP身份验证方式的密码加密传输。

如图12-5所示，在Link Establishment阶段路由器RB要求路由器RA进行身份验证，发送LCP的Configure-Request报文。在Authentication阶段，路由器RA向路由器RB发送Authentication-Request报文，身份验证通过后，路由器RB向路由器RA发送Authentication-Ack报文；如果身份验证失败，RB向RA发送Authentication-Nak报文。图12-5中路由器RA没有要求路由器RB进行身份验证。

如果PPP的Link Establishment阶段顺利结束了，并且PPP的双方约定无须进行认证，或者双方顺利地结束了认证阶段，那么PPP就会自动进入Network Layer Protocol阶段。在Network Layer Protocol阶段，PPP的双方会首先通过NCP来对网络层协议的参数进行协商。协商一致之后，双方才能够在PPP链路上传递携带相应的网络层协议数据单元的PPP帧。

如图12-5所示，在IPCP协商阶段，路由器RA发送的配置请求携带RA的接口IP地址IP-A，如果IP-A是一个合法的单播地址，并且与RB的IP地址不冲突，RB就发送一个IPCP的Configure-Ack报文，如果不认可，则发送一个Configure-Nak报文。

如图12-6所示，如果管理员没有给路由器RA的接口A配置IP地址，而是希望对端设备给接口A分配一个IP地址，那么在IPCP协商阶段，在RA发送的Configure-Request报文的配置选项中就应该包括0.0.0.0这个特殊IP地址。RB收到来自RA的Configure-Request报文后，就会明白对端是在请求从自己这里获取一个IP地址。于是，RB就会回应一个Configure-Nak报文，并把自己分配给接口A的IP地址（假设这个IP地址为IP-A）放在Configure-Nak报文的配置选项中。RA在接收到来自B接口的Configure-Nak报文后，会提取出其中的IP-A，然后重新向B发送一个Configure-Request报文，该报文配置项中包含IP-A。B接收后验证IP-A合法，就会向A发送一个Configure-Ack报文。这样A就成功地从B那里获得了IP-A这个地址。

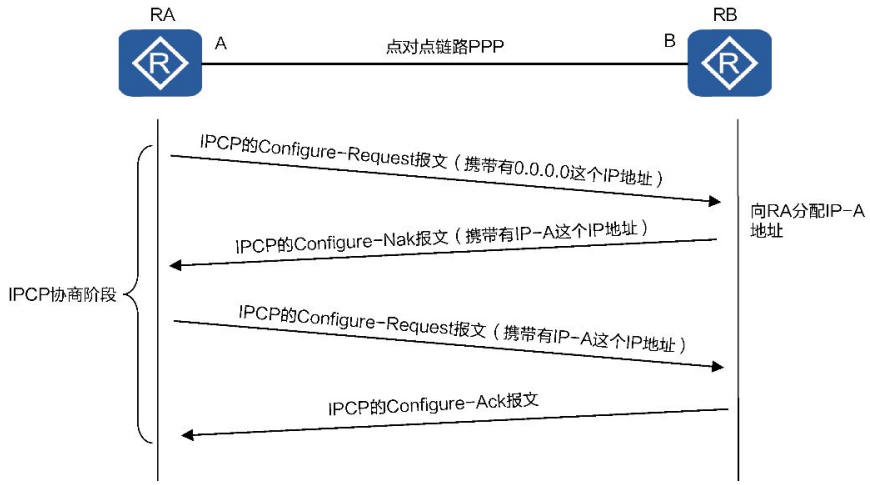


图12-6　RA希望从RB那里获取一个IP地址

有很多情况都会导致PPP进入到Link Termination阶段，例如认证阶段未能顺利完成，链路的信号质量太差，网络管理员需要主动关闭链路等。

12.3　配置PPP

本节配置PPP使用PAP和CHAP两种模式进行身份验证，捕获广域网链路PPP帧，分析PPP帧格式，配置PPP为另一段分配IP地址。本节的实验环境使用eNSP搭建。

12.3.1　配置PPP：身份验证用PAP 模式

如图12-7所示，配置网络中的AR1和AR2路由器实现以下功能。

- 在AR1和AR2之间的链路上进行配置，即将PPP作为数据链路层协议。
- 在AR1上创建用户和密码，用于PPP身份验证。
- 在AR1的Serial 2/0/0接口上，配置PPP身份验证模式为PAP。
- 在AR2的Serial 2/0/1接口上，配置出示给AR1路由器的账号和密码。

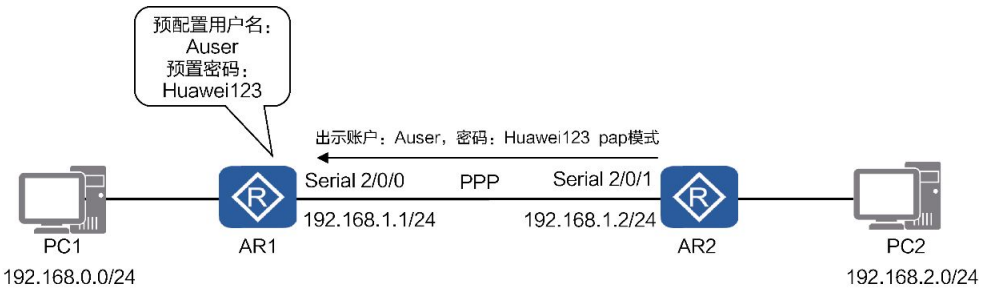


图12-7　PPP实验网络拓扑

在AR1路由器上的Serial 2/0/0接口配置数据链路层使用PPP，华为路由器串行接口默认使用的就是PPP，下面的操作可查看串行接口支

持的数据链路层协议，可以看到同一个接口能够指定使用不同的数据链路层协议。

```
[AR1]interface  Serial  2/0/0
[AR1-Serial2/0/0]link-protocol                          --查看串行接口支持的数据链路层协议
    fr         Select  FR  as  line  protocol
    hdlc     Enable  HDLC  protocol
    lapb     LAPB(X.25  level  2  protocol)
    ppp       Point-to-Point  protocol
    sdlc     SDLC(Synchronous  Data  Line  Control)  protocol
    x25       X.25  protocol
[AR1-Serial2/0/0]link-protocol  ppp
--数据链路层协议指定使用PPP
```

查看AR1路由器上的Serial 2/0/0接口的状态。返回的消息显示物理层状态为UP，表明两端接口连接正常；显示数据链路层状态为UP，表明两端协议一致。

```
<AR1>display  interface  Serial  2/0/0
Serial2/0/0  current  state  :  UP
--物理层状态UP
Line  protocol  current  state  :  UP
--数据链路层状态UP
Description:HUAWEI,  AR  Series,  Serial2/0/0  Interface
Route  Port,The  Maximum  Transmit  Unit  is  1500,  Hold  timer  is  10(sec)
Internet  Address  is  192.168.1.1/24
Link  layer  protocol  is  PPP
--数据链路层协议为PPP
LCP  reqsent
……
```

在AR1上创建用于PPP身份验证的用户。

```
[AR1]aaa
[AR1-aaa]local-user  Auser  password  cipher  Huawei123  --创建用户Auser，密码为Huawei123
[AR1-aaa]local-user  Auser  service-type  ppp                    --
```

```
指定Auser用于PPP身份验证
[AR1-aaa]quit
```

配置AR1接口Serial 2/0/0，PPP要求进行身份验证才能连接，身份验证模式为PAP。

```
[AR1]interface  Serial  2/0/0
[AR1-Serial2/0/0]ppp  authentication-mode  ?                    --查看
PPP身份验证模式
    chap    Enable  CHAP  authentication
--密码安全传输
    pap      Enable  PAP  authentication
--密码明文传输
[AR1-Serial2/0/0]ppp  authentication-mode  pap                --需要
PAP身份验证
```

如果要取消该接口的PPP身份验证，需执行以下命令：

```
[AR1-Serial2/0/0]undo  ppp  authentication-mode  pap
```

在AR2路由器上的Serial 2/0/1接口配置数据链路层使用PPP，并指定向AR1出示的账号和密码。

```
[AR2]interface  Serial  2/0/1
[AR2-Serial2/0/1]link-protocol  ppp
[AR2-Serial2/0/1]ppp  pap  local-user  Auser  password  cipher
Huawei123
```

注意：

在AR2的Serial 2/0/1接口上没有执行[AR2-Serial2/0/1] ppp authentication-mode pap，AR1使用PPP连接RA2时，不需要出示账号和

密码。

12.3.2　配置PPP：身份验证用CHAP模式

上面的配置只是实现了AR1验证AR2。现在要配置AR2验证AR1，在AR2上创建用户Buser，密码为huawei@123。配置AR2的Serial 2/0/1接口使用PPP，要求身份验证，身份验证模式为CHAP。配置AR1的Serial 2/0/0接口出示账号和密码，如图12-8所示。

在AR2上创建PPP身份验证的用户。配置Serial 2/0/1接口，PPP要求完成身份验证才能连接。

```
[AR2]aaa
[AR2-aaa]local-user  Buser  password  cipher  huawei@123
[AR2-aaa]local-user  Buser  service-type  ppp
[AR2-aaa]quit
[AR2]interface  Serial  2/0/1
[AR2-Serial2/0/1]ppp  authentication-mode  chap                    -
-要求完成身份验证才能连接
[AR2-Serial2/0/1]quit
```

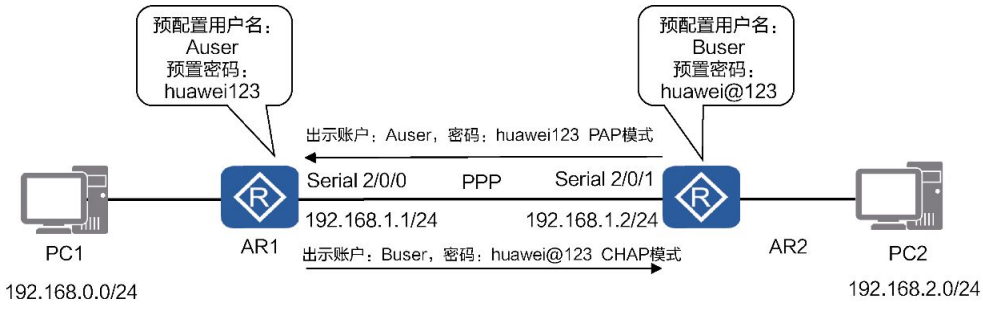


图12-8　配置PPP身份验证用CHAP模式

AR1上的配置如下，先指定用于PPP身份验证的账号，再指定密码。

```
[AR1]interface  Serial  2/0/0
[AR1-Serial2/0/0]ppp  chap  user                          Buser
--账号
[AR1-Serial2/0/0]ppp  chap  password  cipher  huawei@      123
--密码
[AR1-Serial2/0/0]quit
```

12.3.3　抓包分析PPP链路建立过程

通过抓包工具，我们既能捕获计算机通信的数据包，也能捕获PPP建立连接、身份验证、参数协商的数据包。如图12-9所示，右键单击AR2，在出现的菜单中单击“数据抓包”→“Serial 2/0/1”，在出现的“eNSP--选择链路类型”对话框中选择“PPP”，单击“确定”按钮。

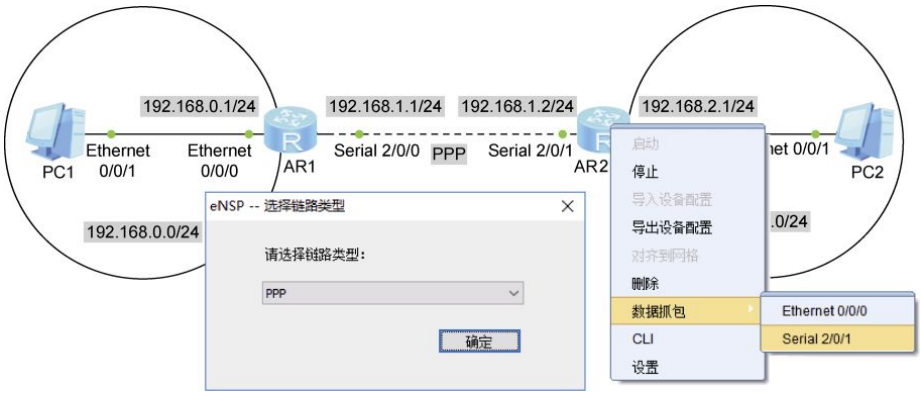


图12-9　抓包分析PPP帧

开始抓包后，禁用AR1路由器的Serial 2/0/0接口，再启用。抓包工具就能捕获PPP建立连接、身份验证、参数协商的数据包。

```
[AR1]interface  Serial  2/0/0
[AR1-Serial2/0/0]shutdown
[AR1-Serial2/0/0]undo  shutdown
```

如图12-10所示，捕获点到点链路的PPP帧，可以看到帧1～5是链路建立阶段发送的帧，使用的协议是PPP LCP。帧6～7是认证阶段发送的帧，使用的协议是PPP PAP。帧8～11是网络层协商阶段发送的帧，使用的协议是PPP IPCP。经过三个阶段建立了PPP链路，就可以发送IP数据包了。图12-10中帧12～18是封装IP数据包。

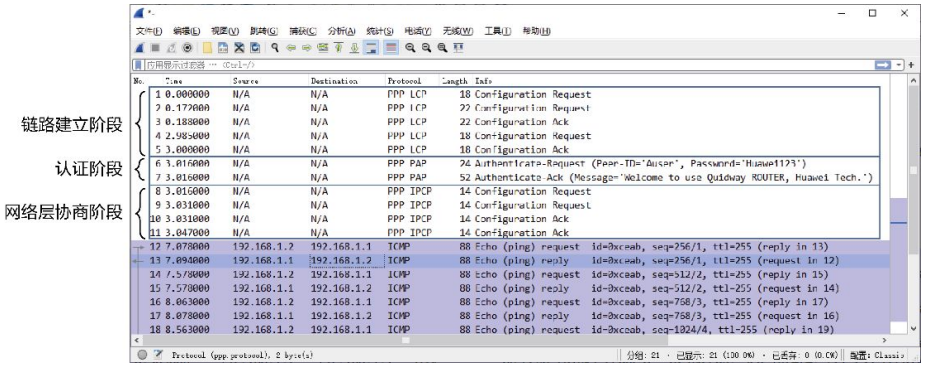


图12-10　PPP链路建立的三个阶段

下面通过观察捕获的PPP建立连接的帧，来分析PPP链路建立的过程。下面描述帧的编号与图12-10捕获的帧的编号相同。

如图12-11所示，第2帧是AR1路由器在链路建立阶段发送的配置请求帧，Protocol为Link Control Protocol（链路控制协议）。Code为Configuration Request（配置请求）。接口参数有3个，Maximum Receive Unit（最大接收单元）为1500、Authentication Protocol为Password Authentication Protocol（密码身份验证协议）、Magic Number（魔术字）为0x328c2356，魔术字由AR1随机产生。

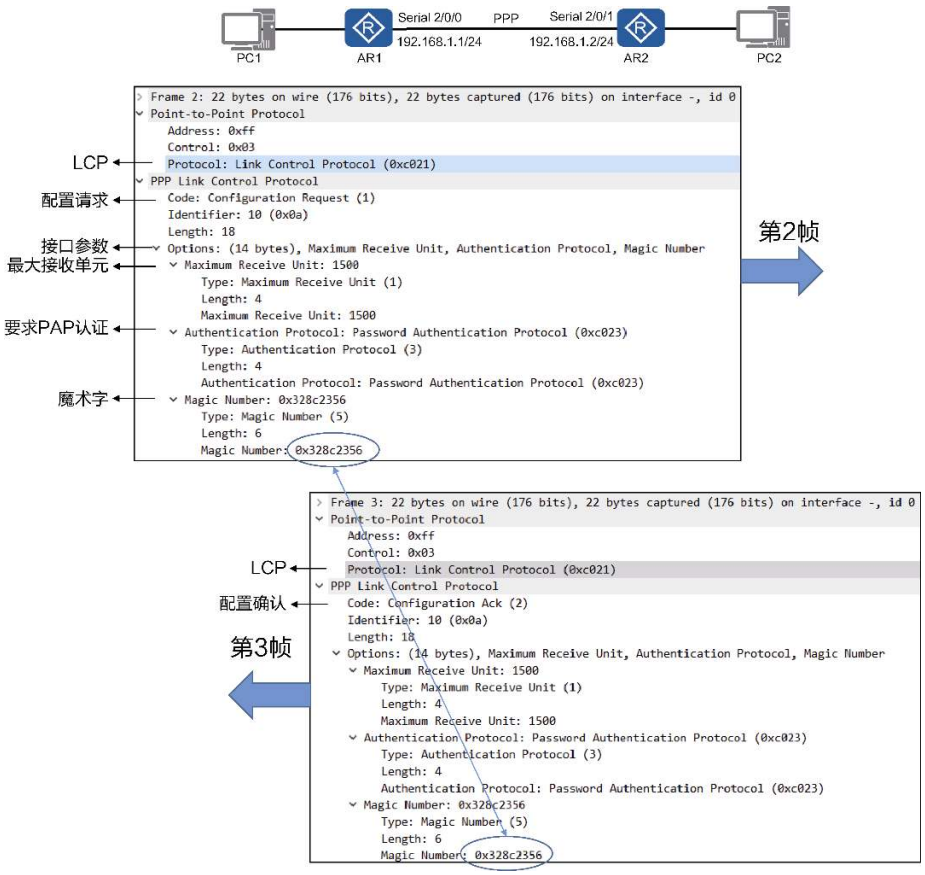


图12-11　链路建立阶段AR1接口参数协商

AR2收到AR1发送的配置请求帧，能够识别并接受这三个参数，然后向AR1发送配置确认帧（第3帧）。注意观察魔术字和第2帧的魔术字一样。这样就能确保第3帧就是第2帧的配置确认帧。可以看到配置确认帧包含了配置请求帧的全部参数。

如图12-12所示，第4帧是AR2向AR1发送配置请求帧，该帧只有两个参数需要和AR1进行协商，即最大接收单元和魔术字。第5帧是AR1向AR2发送的配置确认帧，表示能够识别并接受这两个参数。注意观察第4帧和第5帧的魔术字，也是相同的。

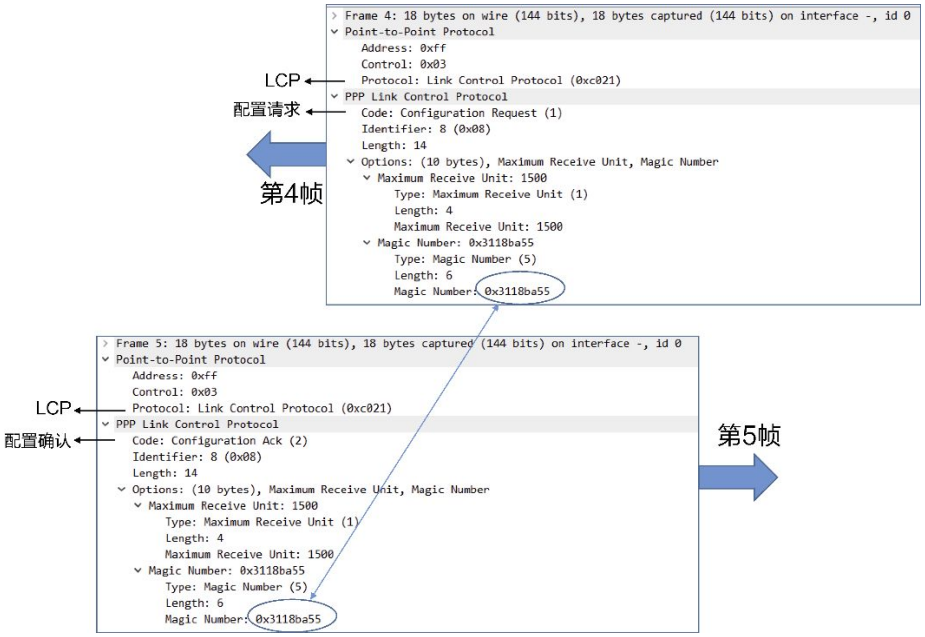


图12-12　链路建立阶段AR2接口参数协商

在链路建立阶段，AR1要求PAP认证，这就进入了认证阶段。如图12-13所示，第6帧是AR2向AR1发送的认证请求，Protocol为Password Authentication Protocol，Data部分包括用户名Auser和密码Huawei123，可以看到账号、密码明文传输。AR1收到认证请求后，验证用户名和密码；通过认证后，发送认证确认帧（第7帧）。

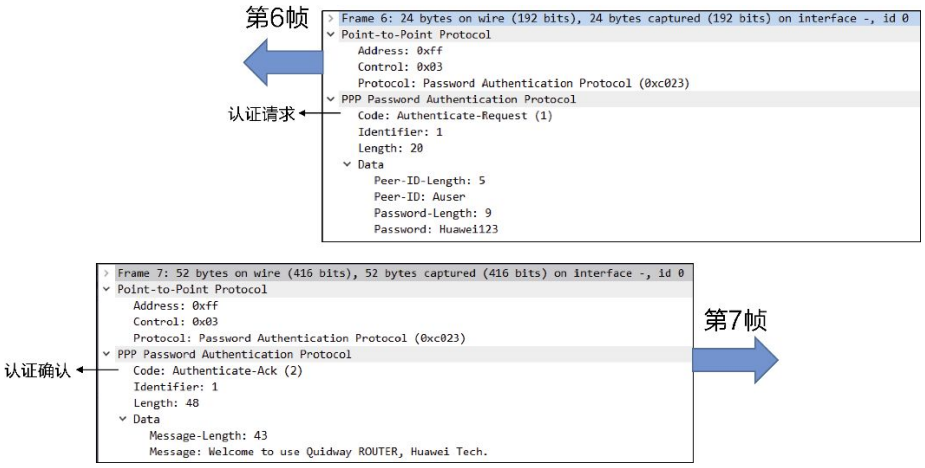


图12-13　认证阶段AR1认证AR2

认证阶段结束后，进入网络层协商阶段。如图12-14所示，第8帧是AR1发送的配置请求帧，注意观察Protocol为Internet Protocol Control Protocol（IPCP），Options包括AR1的Serial 2/0/0接口的IP地址。第9帧是AR1发送的配置请求，注意观察Protocol为Internet Protocol Control Protocol（IPCP），Options包括AR2的Serial 2/0/1接口的IP地址。

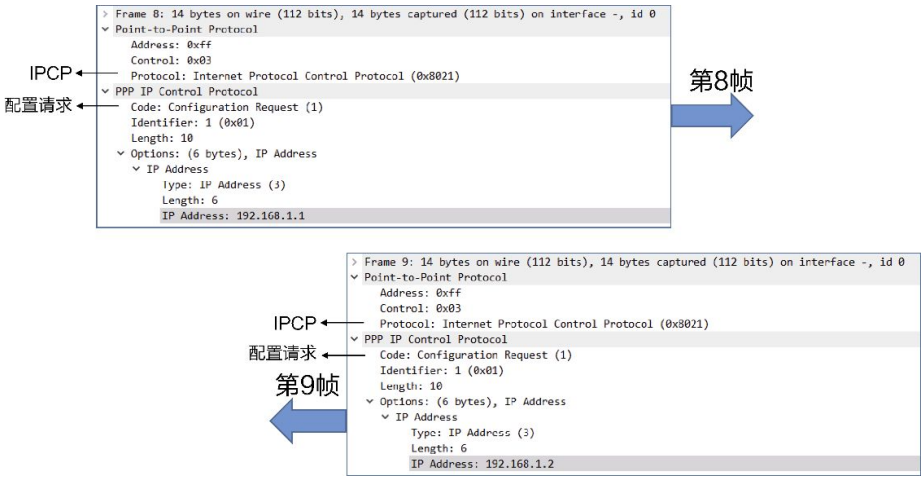


图12-14　网络协商阶段发送配置请求

接收到网络协商发送的配置请求后，计算机就要判断对方出示的IP地址是否和自己的IP地址冲突，以及是否在一个网段。如果地址合法，就给对方发送一个配置确认。如图12-15所示，第10帧是AR2给AR1发送的配置确认，第11帧是AR1给AR2发送的配置确认。

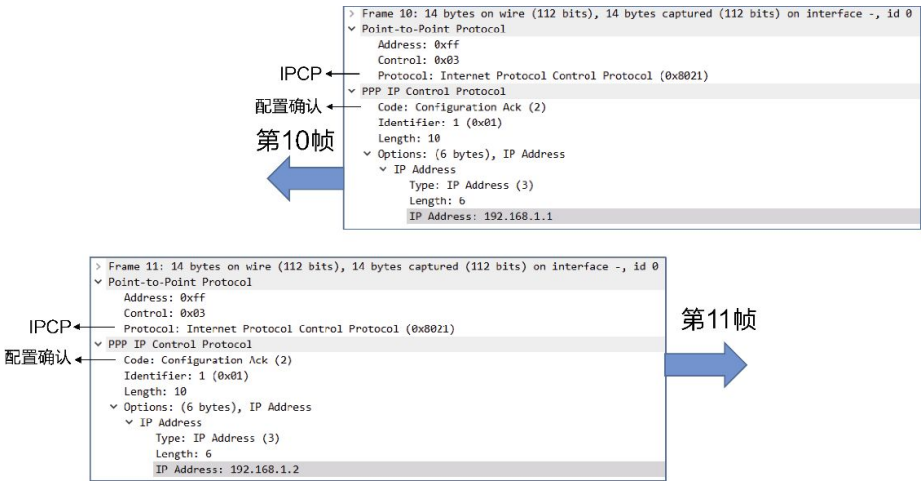


图12-15　网络协商阶段发送配置确认

12.3.4　配置PPP为另一端分配地址

PPP能够为另一端分配地址，这称为动态地址协商。

如图12-16所示，配置AR2为AR1分配IP地址。

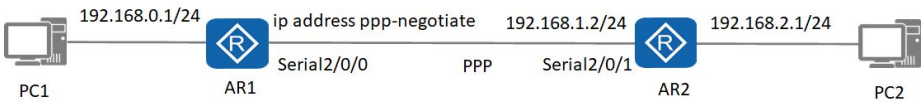


图12-16　动态地址协商实验网络拓扑

在AR1上执行以下命令。

```
[AR1]interface  Serial  2/0/0
[AR1-Serial2/0/0]undo  ip  address
--删除IP地址
[AR1-Serial2/0/0]ip  address  ppp-negotiate                    --配置地
址使用PPP协商
```

在AR2上执行以下命令。另一端地址不固定的话，静态路由最好别写下一跳的IP地址，直接协议出口更合适。

```
[AR2]interface  Serial  2/0/1
[AR2-Serial2/0/1]remote  address  192.168.1.1          --指定给远程分配的地址
[AR2-Serial2/0/1]quit
[AR2]undo  ip  route-static  192.168.0.0  24  192.168.1.1
[AR2]ip  route-static  192.168.0.0  24  Serial  2/0/1
```

设置完成后，右键单击AR2，然后单击“数据抓包”→“Serial 2/0/1”，在出现的“eNSP--选择链路类型”对话框中选择“PPP”，单击“确定”，开始抓包。在AR1上禁用、启用Serial 2/0/0接口，可以捕获PPP动态地址协商的过程，如图12-17所示。

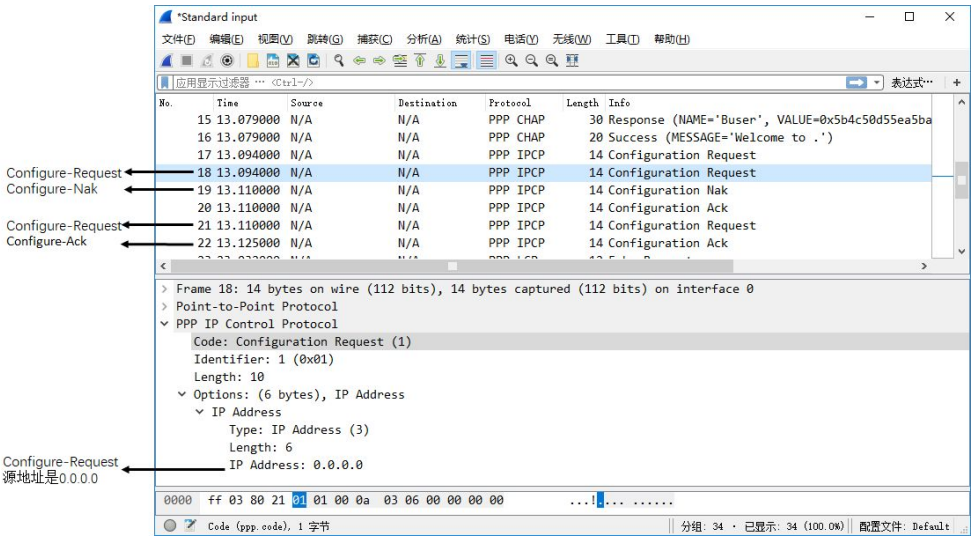


图12-17　动态地址协商的过程

两端动态协商IP地址的过程如下。

（1）AR1向AR2发送一个Configure-Request报文，此报文中会包含一个IP地址0.0.0.0，表示向对端请求IP地址。

（2）AR2收到上述Configure-Request报文后，认为其中包含的地址（0.0.0.0）不合法，使用Configure-Nak回应一个新的IP地址192.168.1.1。

（3）AR1收到此Configure-Nak报文之后，更新本地IP地址，并重新发送一个Configure- Request报文，发报文包含新的IP地址192.168.1.1。

（4）AR2收到Configure-Request报文后，认为其中包含的IP地址为合法地址，回应一个Configure-Ack报文。

同时，AR2也要向AR1发送Configure-Request报文以请求使用地址192.168.1.2，AR1认为此地址合法，回应Configure-Ack报文。

12.4　PPPoE

12.4.1　PPPoE概述

我们先来看一下家庭用户上网的一种典型组网场景，如图12-18所示。在图12-18中，PC1-3以及家庭网关HG-1（注：HG是Home Gateway的简称）组成了一个家庭网络。在这个家庭网络中，终端PC通常是通过常见的标准以太链路或FE链路与HG-1相联。HG-1是家庭网络1的出口网关路由器。为了利用已经铺设好的电话线路，HG-1会利用ADSL（Asymmetric Digital Subscriber Line）技术将自己准备向外发送的以太帧信号调制成一种适合在电话线路上传输的物理信号后再进行发送。网络运营商的IP-DSLAM（IP Digital Subscriber Line Access Multiplexer）设备会接收来自不同HG的ADSL信号，并将其中的以太帧信息解调出来，然后通过一条GE链路将这些以太帧送往一个叫作AC（Access Concentrator）的设备。从数据链路层的角度来看，IP-DSLAM设备就是一台普通的二层以太网汇聚交换机。

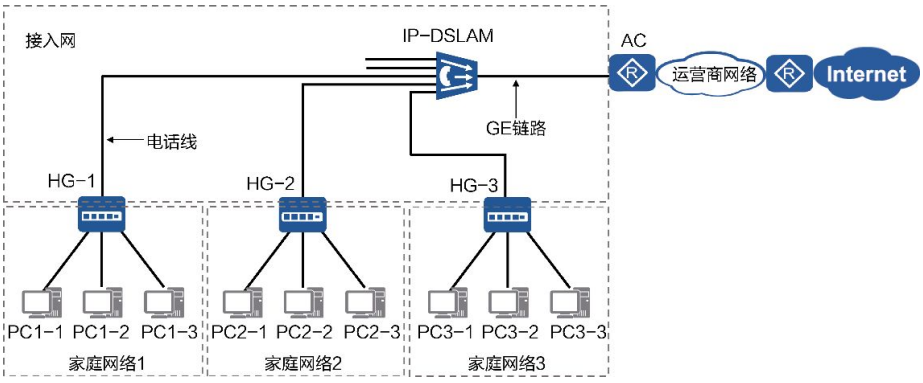


图12-18　家庭用户上网的一种组网场景

我们知道，网络运营商是要对家庭用户上网进行收费的，它还涉及其他一些管理控制行为。然而我们也知道，IP-DSLAM转发给AC的帧是一些以太帧：显然，这些以太帧是无法标识自己是来自HG-I，还是来自HG-2。从帧的结构上来看，一个以太帧中是没有任何字段可以携带“用户名”和“密码”这些信息的。运营商如果不能区分来自不同的家庭用户的数据流量，当然也就无法进行收费等行为了。

因此，在图12-18中，AC设备必须根据所接收的以太帧来识别这些帧所对应的家庭用户，并采用用户名和密码的形式来对不同的家庭用户进行认证。在此基础之上，运营商才有可能对家庭用户的上网活动进行计费等管理控制行为。

我们知道，PPP本身就具备了通过用户名和密码的形式进行认证的功能。然而，PPP只适用于点到点的网络类型。在图12-18中，不同的HG和AC构成的以太网是一个多点接入网络（Multi-AccessNetwork)，因此PPP无法直接应用在这样的网络上。为了将PPP应用在以太网上，一种被称为PPPoE的协议便应运而生。

从本质上讲，PPPoE（PPP over Ethernet）是一个允许在以太广播域中的两个以太接口之间创建点对点隧道的协议，它描述了如何将PPP帧封装在以太帧中。从PPPoE的角度来看，图12-18中的接入网部分可以简化为图12-19所示的网络。

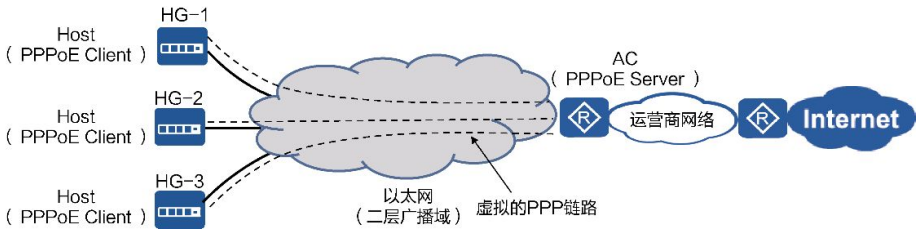


图12-19　从PPPoE的角度来看接入网

在图12-19中，利用PPPoE，每个家庭用户的HG都可以与AC建立起一条虚拟的PPP链路（逻辑意义上的PPP链路）。也就是说，HG与AC是可以交互PPP帧的。然而，这些PPP帧并非是在真实的物理PPP链路上传递的，而是被包裹在HG与AC交互的以太帧中，并随这些以太帧在以太链路上的传递而传递的。

图12-19显示了PPPoE的基本架构。PPPoE采用了Client/Server模式。在PPPoE的标准术语中，运行PPPoE Client程序的设备称为Host，运行PPPoE Server程序的设备称为AC。例如，图12-19中，家庭网关路由器HG就是Host，而运营商路由器就是AC。

12.4.2　PPPoE报文格式

PPP不支持以太网环境，以太网网络适配器接口不可能直接把封装好的PPP数据帧执行成帧操作，然后发送到以太网中。于是，人们想到了一种方法：在封装好的PPP数据帧外面再封装一层以太网数据帧，然后再把这个嵌套了PPP数据帧的以太网数据帧放到以太网中进行传输。这样一来，当运营商的接收方设备接收到这个以太网数据帧时，会通

过解封装发现其中封装的PPP数据帧，然后再根据这个PPP数据帧内部封装的协议，来对数据帧进行相应的处理。

图 12-20 显示了PPPoE报文的格式。如果以太帧的类型字段的值为0x8863或0x8864，则表明以太帧的载荷数据就是一个PPPoE报文。

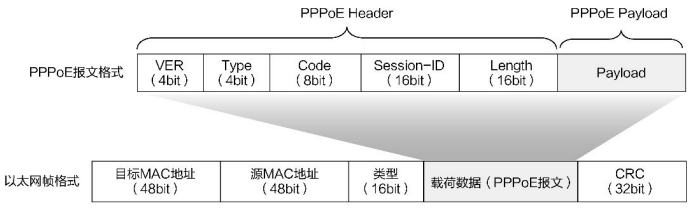


图12-20 PPPoE报文格式

PPPoE报文分为PPPoE Header和PPPoE Payload两个部分。在PPPoE Header中，VER字段（版本字段）的值总是取0x1，Type字段的值也总是取0x1，Code字段用来表示不同类型的PPPoE报文，Length字段用来表示整个PPPoE报文的长度，Session-ID字段用来区分不同的PPPoE会话（PPPoE Session），PPP帧在PPPoE Payload中。

12.4.3 PPPoE的工作过程

PPPoE的工作过程分为两个不同的阶段，即发现阶段（Discovery阶段）和PPP会话阶段（PPP Session阶段）。

1. 发现阶段

如图12-21所示，在PPPoE发现阶段，Host与AC之间会交互4种不同类型的PPPoE报文，分别是PADI（PPPoE Active Discovery Initiation）报文（PPPoE Header中Code字段的值为0x09）、PADO（PPPoE Active Discovery Offer）报文（PPPoE Header中Code字段的值为0x07）、PADR（PPPoE Active Discovery Request）报文（PPPoE Header中Code字段的值为0x19）、PADS（PPPoE Active Discovery Session-confirmation）报文（PPPoE Header中Code字段的值为0x65）。

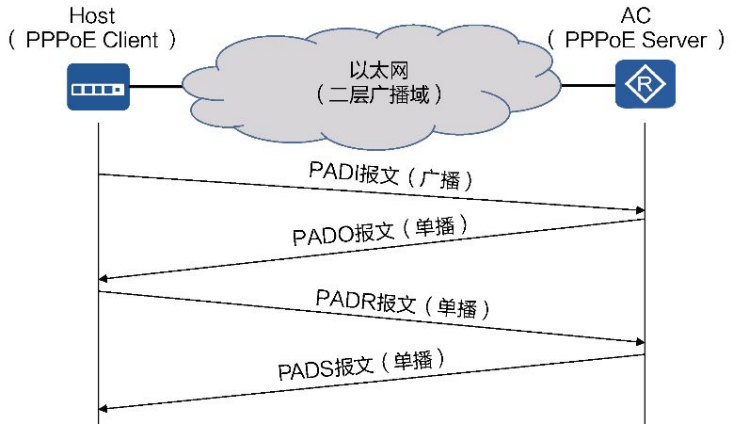


图12-21　PPPoE的发现阶段

首先，Host会以广播的方式发送一个PADI报文（见图12-22），目的是寻找网络中的AC，并告诉AC自己希望获得的服务类型信息。在PADI报文的Payload中，包含的是若干个具有Type-Length-Value结构的Tag字段，这些Tag字段表达了Host想要获得的各种服务类型信息。注意，PADI报文中的Session-ID字段的值为0。

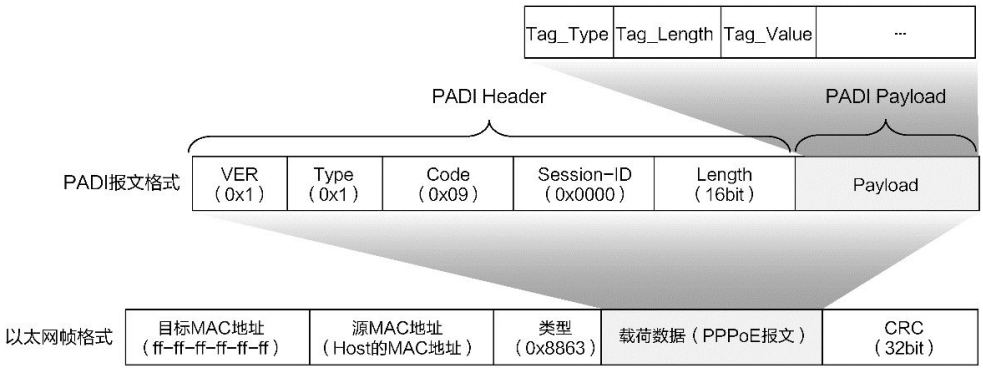


图12-22　PADI报文格式

AC接收到PADI报文之后，会将PADI报文中所请求的服务与自己能够提供的服务进行比较。AC如果能够提供Host所请求的服务，则单播回复一个PADO报文；如果不能提供，则不做任何回应。PADO报文中的Session-ID字段的值为0。

如果网络中有多个AC，则Host就可能接收到来自不同的AC所回应的PADO报文。通常，Host会选择最先收到的PADO报文所对应的AC来作为自己的PPPoE Server，并向这个AC单播发送一个PADR报文。PADR报文中的Session-ID字段的值仍然为0。

AC接收到PADR报文之后，会确定一个PPPoE Session_ID，并在发送给Host的单播PADS报文中携带这个PPPoE Session_lD。PADS报文中的Session-ID字段的值为0x××××，这个值便是PPPoE Session_ID。

Host接收到PADS报文并获知了PPPoE Session_ID之后，便标志着Host与AC之间已经成功建立起了PPPoE会话（PPPoE Session）。接下来，Host和AC便可进入到PPP会话阶段。

2. PPP会话阶段

在PPP会话阶段，Host与AC之间交互的仍然是以太帧，但是这些以太帧携带了PPP帧。图12-23显示了在PPP会话阶段Host与AC之间交互的以太帧所包含的内容。以太帧的类型字段的值为0x8864（注：在发现阶段，以太帧的类型字段的值总是为0x8863），表明以太帧的载荷数据仍然是一个PPPoE报文。在PPPoE报文中，Code字段的值取0x00，Session_ID字段的值保持为在发现阶段所确定的值。现在我们终于可以看到此时的PPPoE报文的Payload就是一个PPP帧！然而，需要注意的是，PPPoE报文的Payload并非是我们之前所熟悉的一个完整的PPP帧，它只是PPP帧的Protocol字段和Information字段。之所以如此，是因为PPP帧的其他字段在此虚拟的PPP链路上已无存在的必要。

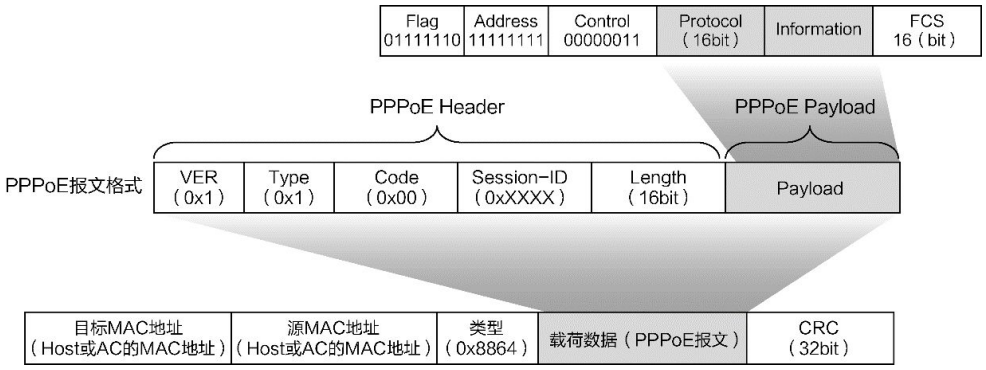


图12-23　携带有PPP帧的以太网帧

可以看到，通过PPPoE协议的中介作用，在PPP会话阶段Host与AC之间就可以交互PPP帧了。通过PPP帧的交互，Host和AC便可经历PPP的链路建立阶段、认证阶段以及网络层协议阶段，最终实现IP报文的交互。

12.4.4 配置Windows PPPoE拨号上网

如图12-24所示，PC1和PC2是某企业内网中的两台计算机，通过交换机LSW1连接到路由器AR1，AR1连接Internet。出于安全考虑，企业内网中的计算机必须验证用户身份后才允许访问Internet。下面展示的实验将AR1路由器配置成PPPoE Server，为企业的每一个用户创建一个拨号的账户和密码。PC1和PC2作为PPPoE Client需要建立PPPoE拨号连接，用户身份验证通过后才能获得一个合法的地址来访问Internet。

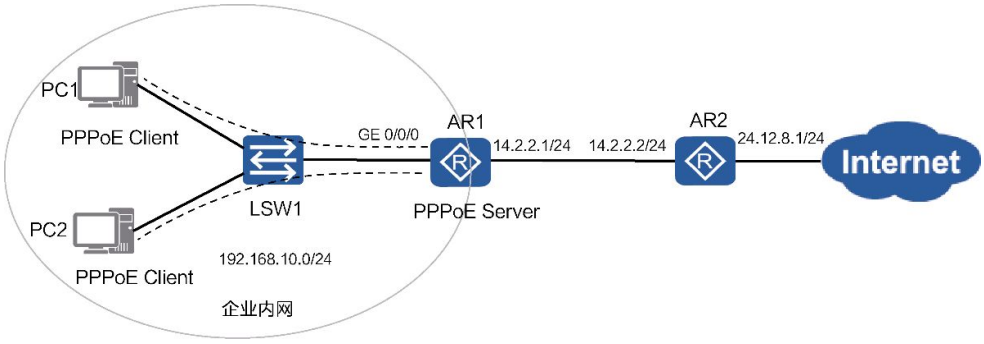


图12-24 PPPoE 实验网络拓扑

首先配置AR1路由器作为PPPoE服务器，并为PC1和PC2创建PPP拨号的账户和密码。

```
[AR1]aaa
[AR1-aaa]local-user hanligang password cipher huawei@123
[AR1-aaa]local-user lishengchun password cipher huawei123
[AR1-aaa]local-user hanligang service-type ppp
[AR1-aaa]local-user lishengchun service-type ppp
[AR1-aaa]quit
```

创建地址池，如果PPPoE拨号成功，则需要给拨号的计算机分配IP地址。

```
[AR1]ip pool PPPoE1
[AR1-ip-pool-PPPoE1]network 192.168.10.0 mask 24
[AR1-ip-pool-PPPoE1]quit
```

创建虚拟接口模板，虚拟接口模板可以绑定到多个物理接口。

```
[AR1]interface Virtual-Template ?
  <0-1023>  Virtual template interface number
[AR1]interface Virtual-Template 1
[AR1-Virtual-Template1]remote address pool PPPoE1        --该虚拟接口给PPPoE client分配的地址池
[AR1-Virtual-Template1]ip address 192.168.10.100 24    --该虚拟接口指定IP地址
[AR1-Virtual-Template1]ppp ipcp dns 8.8.8.8 114.114.114.114 --为PPPoE client指定主、从DNS服务器
[AR1-Virtual-Template1]quit
```

将虚拟接口模板绑定到GigabitEthernet 0/0/0接口，该接口不需要IP地址。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]undo ip address
--去掉配置的IP地址
[AR1-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
--将虚拟接口模板绑定到该接口
[AR1-GigabitEthernet0/0/0]quit
```

一个虚拟接口模板可以绑定PPPoE Server的多个物理接口。

如图12-25所示，路由器AR1有两个以太网接口，连接了两个以太网。这两个以太网中的计算机都要进行PPPoE拨号上网，分配的地址若

都属于192.168.10.0/24这个网段，就可以将虚拟接口模板绑定到这两个物理接口。

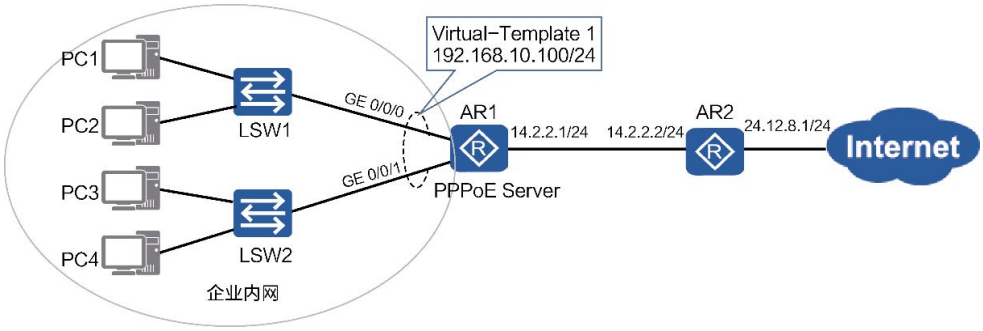


图12-25　将虚拟接口模板绑定物理接口的拓扑图

配置Windows PPPoE拨号上网，就是将Windows计算机配置为PPPoE客户端，也就是在Windows操作系统上创建PPPoE拨号连接，过程如下。

1．登录Windows 10，打开“网络和共享中心”，单击“设置新的连接或网络”。

2．在出现的“选择一个连接选项”对话框中，选中“连接到Internet”，单击“下一步”，然后单击“设置新连接”。

3．在出现的“你希望如何连接”的对话框中单击“宽带（PPPoE）”。

4．如图12-26所示，在出现的“键入您的Internet服务提供商（ISP）提供的信息”对话框中，输入用户名、密码以及连接名称，单击“连接”。



图12-26　输入PPPoE拨号用户和密码

拨通之后，在命令提示符下，输入ipconfig /all以查看拨号获得的IP地址和DNS。

```
C:\Users\win10>ipconfig  /all
Windows  IP  配置
     主机名     .............:  win10-PC
     主  DNS  后缀  ............:
     节点类型     .............:  混合
     IP  路由已启用  ...........:  否
     WINS  代理已启用  ..........:  否
  PPP适配器to  Internet:          --PPPoE拨号获得的地址和DNS
     连接特定的  DNS后缀  .......:
     描述...............:  toInternet
     物理地址.............:
     DHCP  已启用  ............:  否
     自动配置已启用...........:  是
     IPv4  地址  .............:  192.168.10.254(首选)
     子网掩码     .............:  255.255.255.255       --PPP拨号获得的
子网掩码都为255.255.255.255
     默认网关.............:  0.0.0.0
     DNS  服务器     ............:  8.8.8.8
                                          114.114.114.114
     TCPIP  上的  NetBIOS     .......:  已禁用
```

在AR1路由器上可以查看有哪些PPPoE客户端拨入，还可以看到PPPoE客户端的MAC地址，也就是RemMAC。

```
<AR1>display  pppoe-server  session  all
SID  Intf                                    State       OIntf
RemMAC                          LocMAC
1       Virtual-Template1:0          UP           GE0/0/0
000c.2920.c578         00e0.fc4d.3146
```

建立了PPPoE拨号连接后，可以抓包分析PPPoE数据包的帧格式。在Windows 10上运行抓包工具开始抓包，并ping 24.12.8.1。如图12-27所示，观察第411个数据包，PPPoE Payload封装了PPPoE Header，又将其封装到以太网数据帧中，类型字段为0x8864。在PPPoE Header封装中可以看到Session_ID为0x0001。

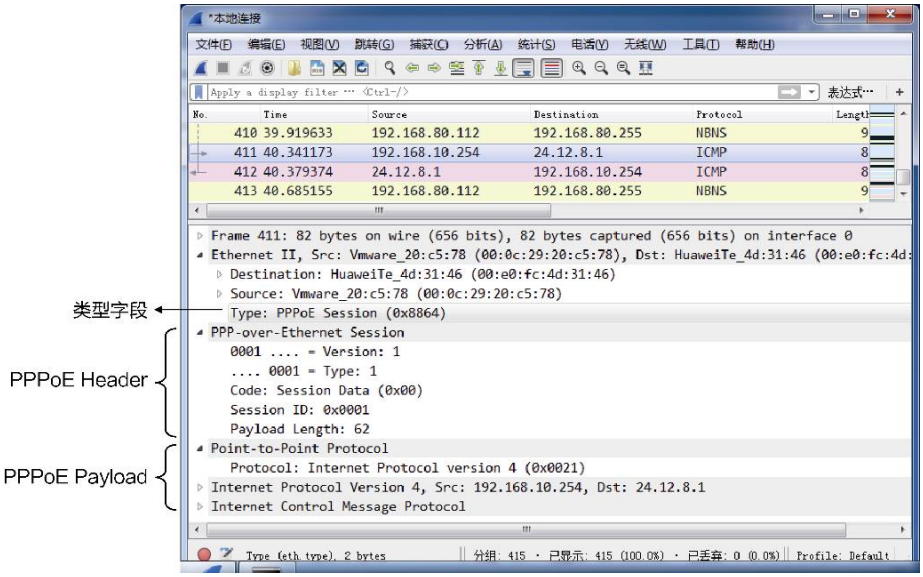


图12-27　查看PPPoE数据包的帧格式

12.4.5　配置路由器PPPoE拨号上网

上面介绍的是将企业的路由器配置为PPPoE服务器，内网的计算机建立PPPoE拨号后访问Internet。更多的情况是企业的路由器连接ADSL Modem接入Internet，这就需要将企业的路由器配置为PPPoE客户端。如图12-28所示，使用eNSP搭建实验环境，没有ADSL Modem，也没有电话线，使用LSW2连接ISP的路由器和学校路由器，将ISP路由器配置为PPPoE服务器，学校A的路由器AR1和学校B的路由器AR2配置为PPPoE客户端，两个学校的内网都属于192.168.10.0/24网段。

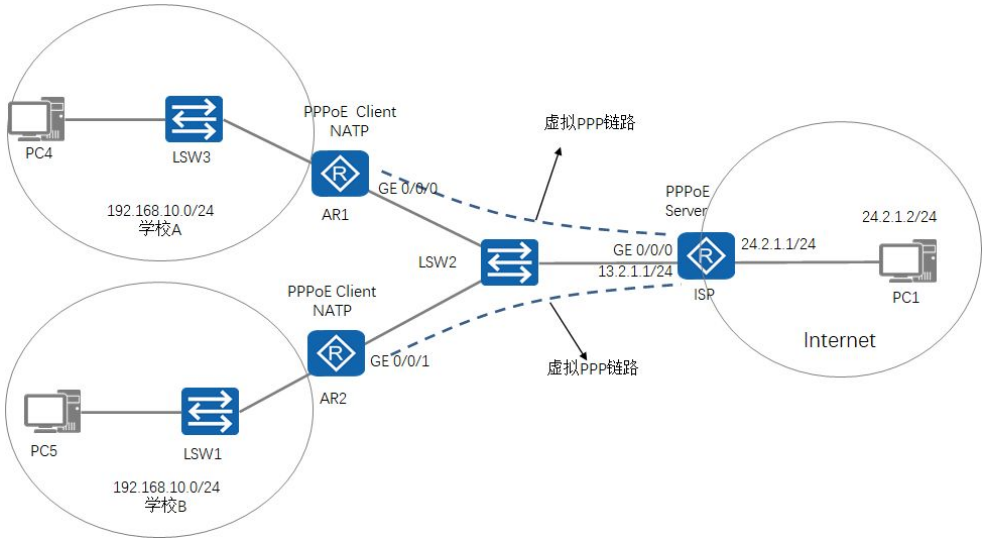


图12-28　配置路由器PPPOE拨号实验拓扑

下面就配置ISP路由器作为PPPoE服务器，配置学校A的AR1路由器作为PPPoE客户端，配置NAPT允许内网访问Internet。

ISP路由器上的配置如下。

创建PPPoE拨号账户，一个学校一个账户。

```
[ISP]aaa
[ISP-aaa]local-user  schoolA  password  cipher  91xueit
```

```
[ISP-aaa]local-user  schoolB  password  cipher  51cto
[ISP-aaa]local-user  schoolA  service-type  ppp
[ISP-aaa]local-user  schoolB  service-type  ppp
[ISP-aaa]quit
```

创建地址池。

```
[ISP]ip  pool  PPPoE1
[ISP-ip-pool-PPPoE1]network  13.2.1.0  mask  24
[ISP-ip-pool-PPPoE1]quit
```

创建虚拟接口模板。

```
[ISP]interface  Virtual-Template  1
[ISP-Virtual-Template1]remote  address  pool  PPPoE1
[ISP-Virtual-Template1]ip  address  13.2.1.1  24
[AR1-Virtual-Template1]ppp  ipcp  dns  8.8.8.8
[ISP-Virtual-Template1]quit
```

将虚拟机接口模板绑定到GE 0/0/0接口。

```
[ISP]interface  GigabitEthernet  0/0/0
[ISP-GigabitEthernet0/0/0]undo  ip  address
[ISP-GigabitEthernet0/0/0]pppoe-server  bind  virtual-template  1
[ISP-GigabitEthernet0/0/0]quit
```

在学校A的路由器上配置PPPoE拨号连接。

创建拨号链路报文过滤规则。

```
[AR1]dialer-rule
[AR1-dialer-rule]dialer-rule  1  ip
[AR11-dialer-rule]dialer-rule  1  ?
    acl      Permit  or  deny  based  on  access-list
    ip        Ip
    ipv6    Ipv6
[AR1-dialer-rule]dialer-rule  1  ip  permit
[AR1-dialer-rule]quit
```

配置某个拨号访问组对应的拨号访问控制列表，指定引发拨号呼叫的条件。创建编号为1的dialer-rule，这个dialer-rule允许所有的IPv4报文通过，同时默认禁止所有的IPv6报文通过。

创建拨号接口Dialer 1，配置接口拨号参数，该接口是逻辑接口。

```
[AR1]interface  Dialer  1
[AR1-Dialer1]link-protocol  ?                                    --
查看支持的协议
    fr      Select  FR  as  line  protocol
    ppp    Point-to-Point  protocol
[AR1-Dialer1]link-protocol  ppp                                  --指定
链路协议为PPP
[AR1-Dialer1]ppp  chap  user  schoolA                           --指定拨
号账户
[AR1-Dialer1]ppp  chap  password  cipher  91xueit --指定拨号密码
[AR1-Dialer1]ip  address  ppp-negotiate                    --地址自动协
商
[AR1-Dialer1]dialer  timer  idle  300                          --如果超
过300秒没有数据传输，断开拨号连接
[AR1-Dialer1]dialer  user  schoolA                               --指定
拨号用户
[AR1-Dialer1]dialer  bundle  1                                    --
这里定义一个  bundle，后面在接口上调用
[AR1-Dialer1]dialer-group  1                                      --
将接口置于一个拨号访问组中
[AR1-Dialer1]quit
```

为拨号接口建立PPPoE会话，如果配置参数on-demand，则PPPoE会话在按需拨号方式下工作。

```
[AR1]interface  GigabitEthernet  0/0/0
[AR1-GigabitEthernet0/0/0]pppoe-client  dial-bundle-number  1  on-
demand
[AR1-GigabitEthernet0/0/0]quit
```

添加默认路由，出口指向Dialer 1接口，这样可以由流量触发PPPoE拨号。

```
[AR1]ip route-static 0.0.0.0 0 Dialer 1                    --由流量触发拨号
[AR1]display dialer interface Dialer 1                     --显示拨号接口状态
Dial Interface:Dialer1
     Dialer Timers(Secs):
     Auto-dial:300        Compete:20        Enable:5
     Idle:120        Wait-for-Carrier:60
```

配置NAPT。

```
[AR1]acl number 2000
[AR1-acl-basic-2000]rule permit source 192.168.10.0 0.0.0.255
[AR1-acl-basic-2000]quit
[AR1]interface Dialer 1
[R1-Dialer1]nat outbound 2000
```

配置完成后，在PC4上ping PC1，测试网络是否畅通。

在AR1路由器上查看拨号接口的状态，可以看到获得的IP地址。

```
<AR1>display interface Dialer 1
Dialer1 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Dialer1 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is negotiated, 13.2.1.254/32
Link layer protocol is PPP
```

12.5　习题

1．下列哪项命令可以用来查看IP地址与帧中继DLCI号的对应关系？（　　）

A．display fr interface

B．display fr map-info

C．display fr inarp-info

D．display interface brief

2．在帧中继网络中，关于DTE设备上的映射信息，描述正确的是（　　）。

A．本地DLCI与远端IP地址的映射

B．本地IP地址与远端DLCI的映射

C．本地DLCI与本地IP地址的映射

D．远端DLCI与远端IP地址的映射

3．在配置PPP验证方式为PAP时，下面哪些操作是必需的？（　　）（选择3个答案）

A．把被验证方的用户名和密码加入验证方的本地用户列表中

B. 将与对端设备相连接口的封装类型配置为PPP

C. 设置PPP的验证模式为CHAP

D. 在被验证方配置向验证方发送的用户名和密码

4. 在华为AR G3系列路由器的串行接口上配置、封装PPP时，需要在接口视图下输入的命令是（　　）。

A. link-protocol ppp

B. encapsulation ppp

C. enable ppp

D. address ppp

5. 两台路由器通过串口连接且数据链路层协议为PPP，如果想在两台路由器上通过配置PPP验证功能来提高安全性，则下列哪种PPP验证更安全？（　　）

A. CHAP

B. PAP

C. MD5

D. SSH

6．在以太网这种多点访问网络中，PPPoE服务器可以通过一个以太网端口与很多PPPoE客户端建立起PPP连接，因此PPPoE服务器必须为每个PPP会话建立唯一的会话标识符以区分不同的连接。PPPoE会使用什么参数建立会话标识符？（　　）

A．MAC地址

B．IP地址与MAC地址

C．MAC地址与PPP-ID

D．MAC地址与Session-ID

7．命令ip address ppp-negotiate有什么作用？（　　）

A．开启向对端请求IP地址的功能

B．开启接收远端请求IP地址的功能

C．开启静态分配IP地址的功能

D．以上选项都不正确

8．PPP由以下哪些协议组成？（　　）（多选）

A．认证协议

B．NCP

C. LCP

D. PPPOE

9. 如果在PPP认证的过程中，被认证者发送了错误的用户名和密码给认证者，认证者将会发送哪种类型的报文给被认证者？（　　）

A. Authenticate-Reject

B. Authenticate-Ack

C. Authenticate-Nak

D. Authenticate-Reply

10. PPP定义的是OSI参考模型中哪个层次的封装格式？（　　）

A. 网络层

B. 数据链路层

C. 表示层

D. 应用层

11. PPPoE客户端向Server发送PADI报文，Server回复PADO报文。其中，PADO报文是一个什么帧？（　　）

A. 组播

B. 广播

C. 单播

D. 任播

第13章　VPN

本章内容

- 虚拟专用网络
- 配置GRE隧道VPN
- 配置IPSec VPN
- 配置基于Tunnel接口的IPSec VPN
- 远程访问VPN

本章介绍虚拟专用网络，在路由器上配置站点间VPN，即通过Internet实现公司异地私有网络的互联互通。本章还展示实现站点间VPN的3种类型VPN，即GRE隧道实现的站点间VPN、IPSec VPN和基于Tunnel接口的IPSec VPN。本章最后展示在路由器上配置远程访问VPN的过程，远程访问VPN允许公司网络外的用户（计算机）建立到公司内网的VPN拨号连接，并通过Internet访问企业私有网络。

13.1　虚拟专用网络

13.1.1　专用网络

在讲虚拟专用网络（Virtual Private Network，VPN）之前，先介绍一下什么是专用网络。

专用网络也就是专线业务，大多面向企业、政府以及其他对带宽稳定性和服务质量要求高的客户。一般具有固网IP地址，不需要进行接入认证；根据客户需求，不仅在接入层对带宽和接入业务类型有要求，而且会对业务的全程、全网服务质量提出更详细的要求；而专线客户，往往由运营商提供更为主动、周全、及时、专业的客户服务支撑。

一家公司异地的局域网可以通过专线连接，如图13-1所示，北京、上海两个城市的局域网可以通过数字数据网（DDN）专线业务、帧中继（FR）专线业务、数字用户线路（DSL）专线业务、同步数字（SDH）专线业务等进行连接。

专线连接的优点为成本高、通信质量好。专线通常用于内网通信，全网通常采用私有IP地址。

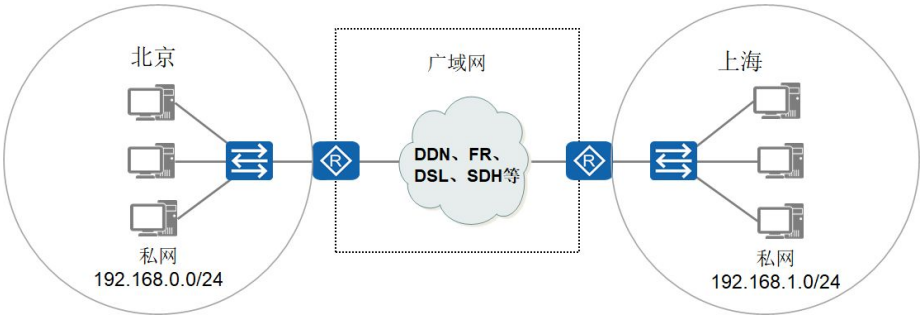


图13-1　专用网络示意图

13.1.2　虚拟专用网络

如图13-2所示，企业在北京的网络接入了Internet，在上海的网络也接入了Internet，这两个局域网通过Internet连接起来，但由于北京和上海的两个网络均是私网，因此不能通过Internet直接相互通信。

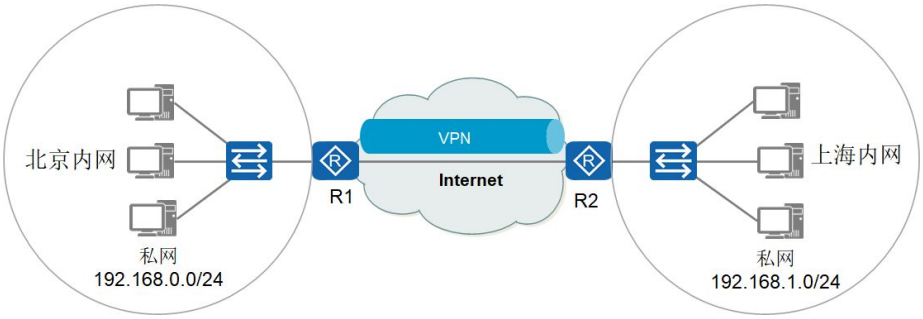


图13-2　VPN示意图

通过配置两端的路由器R1和R2，可以为两个局域网创建一条隧道，让两个局域网之间能够相互通信。通过加密和身份验证技术可以实现数据通信的安全，从而达到像专线一样的效果。这种在公共网络

中建立的连接多个局域网的隧道就称为虚拟专用网络（VPN），如图13-2所示。

通过VPN，用户可利用Internet对两地的网络进行互联，只需要支付本地接入Internet的费用即可，该费用较低。使用IPSec能够保证数据通信安全，可以在不改变使用习惯的前提下，使用私网地址和对方进行通信。

13.2　配置站点间VPN

站点间VPN就是在Internet上创建VPN隧道，以对多个局域网进行连接。本书重点讲GRE隧道和IPSecVPN，如图13-3所示。后面还会讲到远程访问VPN，在远程计算机上建立到企业内网的VPN连接，从而访问企业内网。

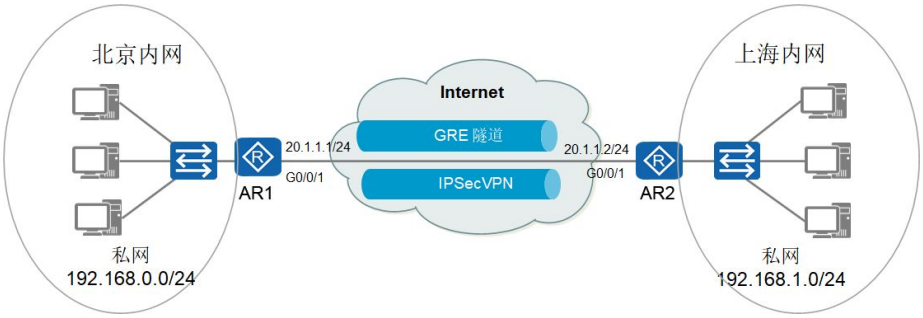


图13-3　VPN隧道

13.2.1　GRE隧道VPN

GRE（Generic Routing Encapsulation）是指通用路由封装协议，它对某些网络层协议（如IP和IPX）的数据包进行封装，使这些被封装的数据包能够在另一个网络层协议（如IP）中传输。下面讨论的GRE隧道VPN，用于将跨Internet内网进行通信的数据包封装到具有公网地址的数据包中进行传输。

如图13-3所示，北京和上海的两个局域网通过Internet连接。在AR1和AR2上配置GRE隧道，这时候大家应该把这条隧道当成连接AR1和AR2的一根网线。AR1隧道接口的地址和AR2隧道接口的地址在同一个网

段。这样理解，就很容易想到，要想实现这两个私网间的通信，需要添加静态路由。在AR1上添加到上海网段的路由，下一跳地址是172.16.0.2；在AR2上添加到北京网段的路由，下一跳地址是172.16.0.1。

图13-4展示了PC1与PC2通信的数据包在隧道中（也就是在Internet中）传输时的封装格式示意图。可以看到，PC1到PC2的数据包的外面又有一层GRE封装，最外面的是隧道的目标地址和源地址。

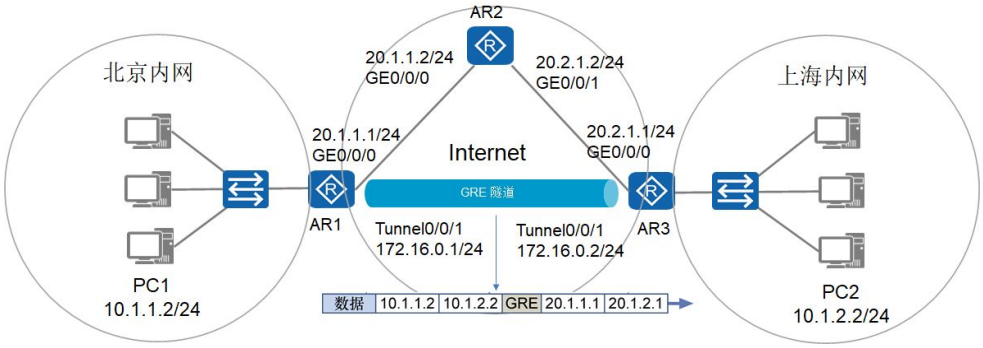


图13-4　GRE隧道VPN的网络拓扑

使用eNSP参照图13-4搭建实验环境。

AR1上的配置如下。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ip address 20.1.1.1 24
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface Vlanif 1
[AR1-Vlanif1]ip address 10.1.1.1 24
[AR1-Vlanif1]quit
[AR1]ip route-static 20.1.2.0 24 20.1.1.2          --添加到
20.1.2.0/24网络的路由
```

AR2上的配置如下，不添加到北京和上海网络的路由，因为Internet中的路由器不会添加到私有网络的路由。

```
[AR2]interface GigabitEthernet 0/0/0
[AR2-GigabitEthernet0/0/0]ip address 20.1.1.2 24
[AR2-GigabitEthernet0/0/0]quit
[AR2]interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1]ip address 20.1.2.2 24
[AR2-GigabitEthernet0/0/1]quit
```

AR3上的配置如下。

```
[AR3]interface GigabitEthernet 0/0/0
[AR3-GigabitEthernet0/0/0]ip address 20.1.2.1 24
[AR3-GigabitEthernet0/0/0]quit
[AR3]interface Vlanif 1
[AR3-Vlanif1]ip address 10.1.2.1 24
[AR3-Vlanif1]quit
[AR3]ip route-static 20.1.1.0 24 20.1.2.2      --添加到20.1.1.0/24网络的路由
```

现在，在AR1上创建到上海网络的GRE隧道接口，并添加到上海网络的路由。

```
[AR1]interface Tunnel 0/0/0                    --指定隧道接口编号
[AR1-Tunnel0/0/0]tunnel-protocol ?             --查看隧道支持的协议
  gre         Generic Routing Encapsulation
  ipsec       IPSEC Encapsulation
  ipv4-ipv6   IP over IPv6 encapsulation
  ipv6-ipv4   IPv6 over IP encapsulation
  mpls        MPLS Encapsulation
  none        Null Encapsulation
[AR1-Tunnel0/0/0]tunnel-protocol gre           --隧道使用GRE协议
[AR1-Tunnel0/0/0]ip address 172.16.0.1 24      --指定隧道接口的地址
[AR1-Tunnel0/0/0]source 20.1.1.1               --指定隧道的起点（源地址）
[AR1-Tunnel0/0/0]destination 20.1.2.1          --指定隧道的终点（目标地址）
[AR1-Tunnel0/0/0]quit
[AR1]ip route-static 10.1.2.0 24 172.16.0.2    --添加到上海网络的路由
```

添加到上海网络的路由，下一跳地址也可以使用Tunnel 0/0/0替换。

```
[AR1]ip route-static 10.1.2.0 24 Tunnel 0/0/0。
```

在AR3上创建到北京网络的GRE隧道接口，并添加到北京网络的路由。

```
[AR3]interface Tunnel 0/0/0
[AR3-Tunnel0/0/0]tunnel-protocol gre
[AR3-Tunnel0/0/0]ip address 172.16.0.2 24
[AR3-Tunnel0/0/0]source 20.1.2.1
[AR3-Tunnel0/0/0]destination 20.1.1.1
[AR3-Tunnel0/0/0]quit
[AR3]ip route-static 10.1.1.0 24 172.16.0.1
```

查看Tunnel 0/0/0接口的状态。

```
<AR3>display interface Tunnel 0/0/0
Tunnel0/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2018-06-16 01:37:01 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 172.16.0.2/24
Encapsulation is TUNNEL, loopback not set
……
```

抓包分析GRE隧道中的数据包格式。如图13-5所示，右键单击AR2路由器，在弹出的菜单中单击“数据抓包”，再单击“GE 0/0/0”接口。

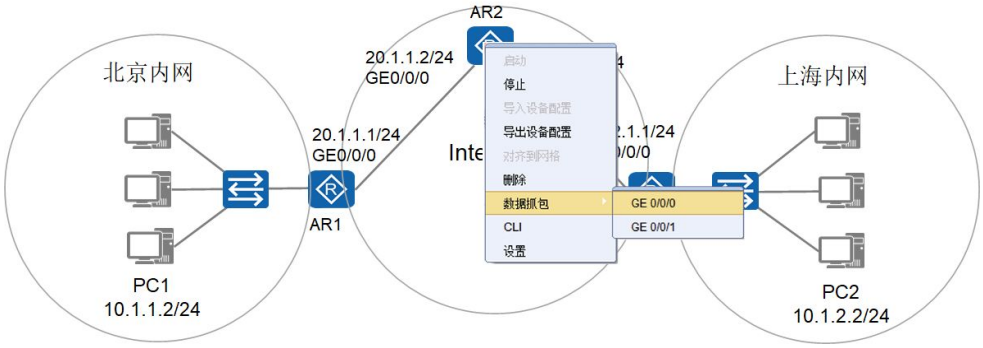


图13-5　抓包分析GRE隧道中的数据包格式

开始抓包后，用PC1 ping PC2，观察捕获的数据包，并查看GRE封装，如图13-6所示。

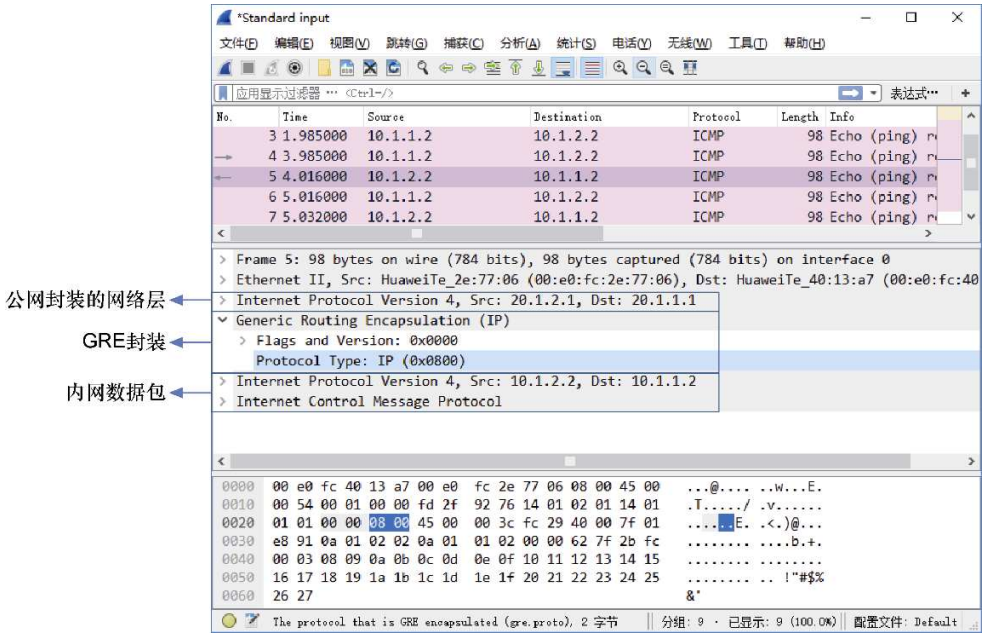


图13-6　查看GRE封装的数据包格式

上面展示了如何创建GRE隧道VPN以将两个城市的局域网连接起来。如果一个企业在北京、上海、石家庄3个城市都有局域网，如图13-7所示。要创建GRE隧道VPN，需要在每个路由器上创建两个Tunnel

接口，分别定义好隧道的起点和终点以及隧道接口地址，并添加到远程网络的路由。

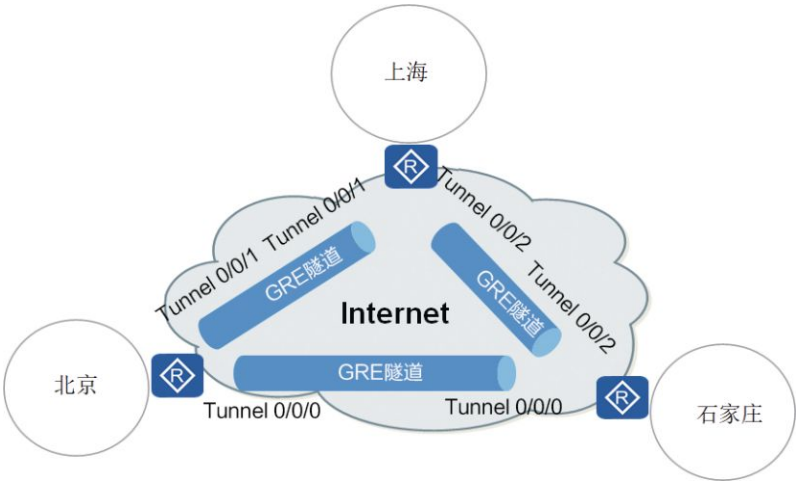


图13-7　创建多GRE隧道以连接多个局域网

总结：GRE是一个标准协议，支持多种协议和多播，能够用来创建弹性的VPN，支持多点隧道，能够实施QoS。

GRE协议存在的问题有：缺乏加密机制，没有标准的控制协议来保持GRE隧道（通常使用协议和keep alive），隧道很消耗CPU，出现问题时进行调试很困难。

13.2.2　介绍IPSec VPN

IPSec（IP Security）是IETF制定的三层隧道加密协议，它为Internet上传输的数据提供高质量的、可互操作的、基于密码学的安全保证。特定的通信方之间在IP层通过加密与数据源认证等方式，提供以下安全服务。

- 数据机密性（data confidentiality）：IPSec发送方在通过网络传输包前对包进行加密。
- 数据完整性（data integrity）：IPSec接收方对发送方发来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证（data authentication）：IPSec在接收端可以认证发送IPSec报文的发送端是否合法。
- 防重放（anti-replay）：IPSec接收方可检测并拒绝接收过时或重复的报文。

IPSec有两种工作模式：传输模式和隧道模式。

如图13-8所示，IPSec传输模式能实现点到点安全通信，IPSec隧道的起点和终点是通信的两台计算机。

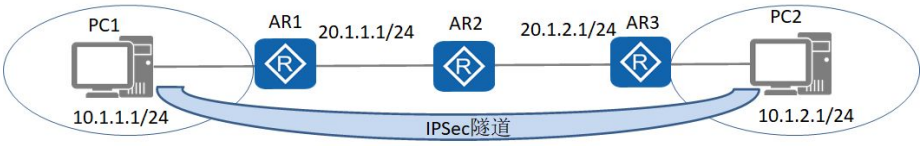


图13-8　IPSec传输模式示意图

如图13-9所示，IPSec隧道模式在AR1和AR3之间配置IPSec隧道，实现网络1和网络2之间的安全通信，图13-9标注了PC2发送给PC4的数据包。查看图13-9，可以看到PC2访问PC4的数据包经过加密认证后又使用隧道的起点和终点地址进行了封装。

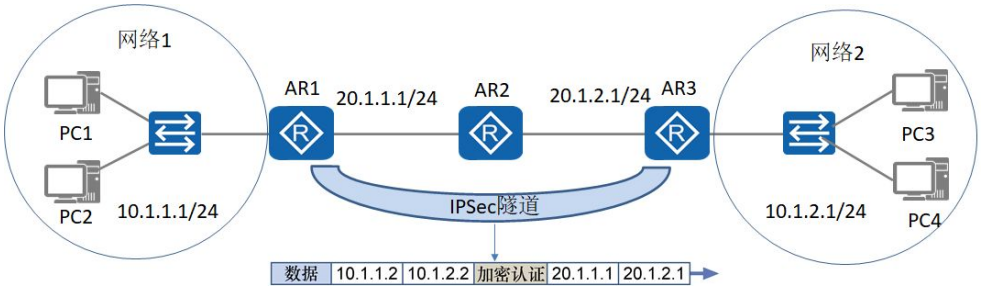


图13-9　IPSec隧道模式示意图

IPSec隧道模式的这种数据包封装方式，正好可以被用于通过Internet连接两个局域网，对在局域网中通信的数据包进行二次封装，以实现局域网的跨Internet通信。通过IPSec隧道模式建立两个局域网间的安全隧道，这就是IPSec VPN。

13.2.3　配置IPSec VPN

下面就使用eNSP搭建图13-10所示的网络环境，在AR1和AR3上配置IPSec隧道，使得北京和上海的网络能够跨Internet通信。

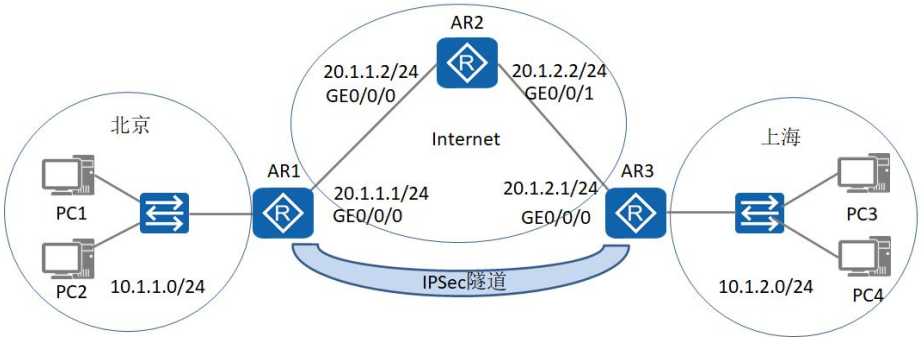


图13-10　IPSec VPN网络拓扑

配置IPSec VPN时，需要在AR1和AR3路由器上进行以下配置。

（1）定义需要保护的数据流，这里采用高级ACL，对要保护的数据流的源/目的IP地址等信息进行限制，仅允许指定的数据流进入IPSec隧道中传输。

（2）确定IPSec安全提议，定义加密通信两端所采用的安全参数（AH或ESP，或同时都选用）、认证算法（MD5、SHA-1、SHA-2）、加密算法（DES、3DES、SM1）和报文封装格式（传输模式或隧道模式）。

（3）创建Internet密钥交换（Internet Key Exchange，IKE）对等实体，指定隧道的终点地址和进行身份验证的预共享密钥。

（4）配置安全策略，它是两端建立安全联盟（Security Association，SA）的基础信息，包括引用前面定义的数据流保护ACL和IPSec安全提议，配置IPSec隧道的起点和终点IP地址，SA出/入方向的SPI值以及SA出/入方向安全协议的认证密钥和加密密钥。

（5）在接口上应用安全策略。

（6）添加到远程网络的路由。

AR1上的配置如下。

定义要保护的数据流（感兴趣流）。

```
[AR1]acl 3000
[AR1-acl-adv-3000]rule permit ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0
0.0.0.255
[AR1-acl-adv-3000]rule deny ip
[AR1-acl-adv-3000]quit
```

确定IPSec安全提议。

```
[AR1]ipsec proposal prol     --创建安全提议，名为prol
[AR1-ipsec-proposal-prol]esp authentication-algorithm sha1    --指定
身份验证算法
[AR1-ipsec-proposal-prol]esp encryption-algorithm aes-128     --指定
数据加密算法
[AR1-ipsec-proposal-prol]quit
[AR1]display ipsec proposal name prol                         --查看
定义的安全提议
IPSec proposal name: prol
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA1-HMAC-96      Encryption
AES-128
```

创建IKE对等实体。

```
[AR1]ike peer toshanghai v1                                   --指定对等实
体的名称和版本
[AR1-ike-peer-toshanghai]pre-shared-key simple 91xueit  --预共享密钥
为91xueit
[AR1-ike-peer-toshanghai]remote-address 20.1.2.1        --隧道的终点
IP地址
[AR1-ike-peer-toshanghai]quit
```

创建IPSec安全策略。

```
[AR1]ipsec policy policy1 10 ?                          --策略名为
policy1，指定索引号10
  isakmp  Indicates use IKE to establish the IPSec SA  --使用IKE建
立IPSec安全联盟
  manual  Indicates use manual to establish the IPSec SA --人工建立
IPSec安全联盟
  <cr>    Please press ENTER to execute command
[AR1]ipsec policy policy1 10 isakmp
[AR1-ipsec-policy-isakmp-policy1-10]ike-peer toshanghai --指定IKE对
等实体
[AR1-ipsec-policy-isakmp-policy1-10]proposal prol     --指定安全提议
[AR1-ipsec-policy-isakmp-policy1-10]security acl 3000 --指定感兴趣流
[AR1-ipsec-policy-isakmp-policy1-10]quit
```

把IPSec绑定到物理接口。

```
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ipsec policy policy1
[AR1-GigabitEthernet0/0/0]quit
```

添加到上海网络的路由，注意：下一跳地址是路由器AR1的GE 0/0/0接口地址。

```
[AR1]ip route-static 20.1.2.0 24 20.1.1.2
[AR1]ip route-static 10.1.2.0 24 20.1.1.2
```

AR3上的配置如下。

定义要保护的数据流。

```
[AR3]acl 3000
[AR3-acl-adv-3000]rule permit ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[AR3-acl-adv-3000]rule deny ip
[AR3-acl-adv-3000]quit
```

确定IPSec安全提议。

```
[AR3]ipsec proposal prol
[AR3-ipsec-proposal-prol]esp authentication-algorithm sha1
[AR3-ipsec-proposal-prol]esp encryption-algorithm aes-128
[AR3-ipsec-proposal-prol]quit
```

创建IKE对等实体。

```
[AR3]ike peer tobeijing v1
[AR3-ike-peer-tobeijing]pre-shared-key simple 91xueit  --这个密钥一
定要和AR1定义的相同
[AR3-ike-peer-tobeijing]remote-address 20.1.1.1
[AR3-ike-peer-tobeijing]quit
```

创建IPSec安全策略。

```
[AR3]ipsec policy policy1 10 isakmp
[AR3-ipsec-policy-isakmp-policy1-10]ike-peer tobeijing
[AR3-ipsec-policy-isakmp-policy1-10]proposal prol
[AR3-ipsec-policy-isakmp-policy1-10]security acl 3000
[AR3-ipsec-policy-isakmp-policy1-10]quit
```

把IPSec绑定到物理接口。

```
[AR3]interface GigabitEthernet 0/0/0
[AR3-GigabitEthernet0/0/0]ipsec policy policy1
[AR3-GigabitEthernet0/0/0]quit
```

添加到上海网络的路由，注意：下一跳地址是路由器AR1的GE 0/0/0接口地址。

```
[AR3]ip route-static 20.1.1.0 24 20.1.2.2
[AR3]ip route-static 10.1.1.0 24 20.1.2.2
```

抓包分析IPSec隧道中的数据包格式。如图13-11所示，右键单击AR2路由器，在弹出的菜单中单击“数据抓包”，再单击“GE 0/0/0”接口。

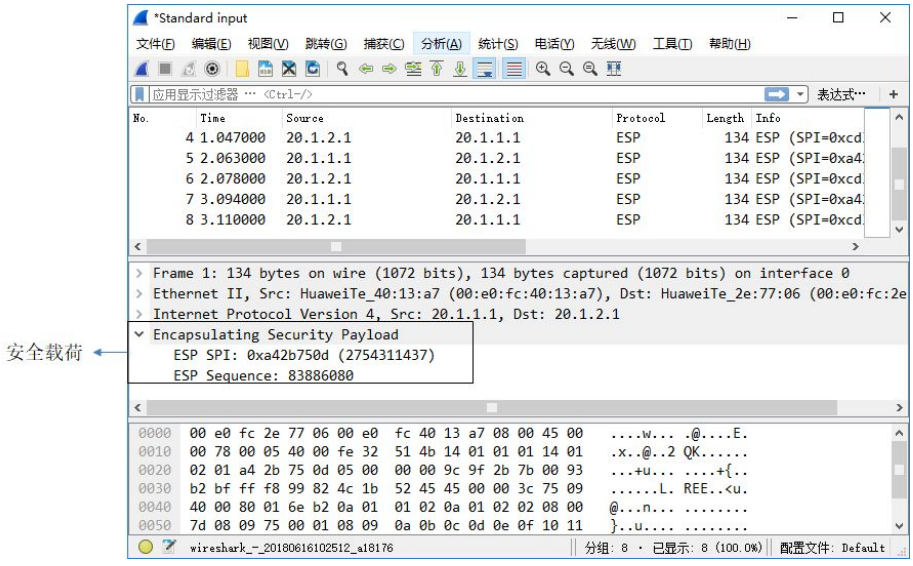


图13-11　IPSec VPN数据包结构

开始抓包后，用PC1 ping PC2，观察捕获的数据包，然后查看IPSec隧道中的数据包，可以看到PC1发送给PC2中的数据包被封装在安全载荷中，但不能看到数据包的内网地址信息。

13.2.4　基于Tunnel接口的IPSec VPN

还有一种IPSecVPN，就是基于Tunnel接口的IPSec VPN。先创建连接局域网的隧道接口，添加到局域网的路由，再将IPSec策略绑定到隧道接口，这就不用使用ACL确定对哪些数据流进行IPSec保护了。

实验环境如图13-12所示，在AR1和AR3上配置基于Tunnel接口的IPSec VPN，通过Internet连接北京和上海的两个网络。

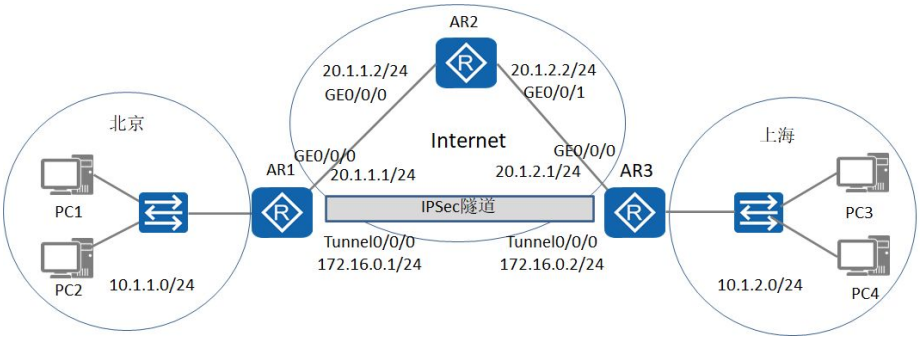


图13-12　基于Tunnel接口的IPSec VPN网络拓扑

AR1上的配置如下。

```
[AR1]ipsec proposal prop                                    --创建安全提议，名为prop
[AR1-ipsec-proposal-prop]quit                               --使用默认参数
```

```
[AR1]ike peer toshanghai v2                                    --创建IKE对
等实体
[AR1-ike-peer-toshanghai]peer-id-type ?
  ip    Select IP address as the peer ID
  name  Select name as the peer ID
[AR1-ike-peer-toshanghai]peer-id-type ip                       --选择IP地
址作为对等ID
[AR1-ike-peer-toshanghai]pre-shared-key simple 91xueit         --指定预共享
密钥
[AR1-ike-peer-toshanghai]quit

[AR1]ipsec profile profile1                                    --创建安全框
架
[AR1-ipsec-profile-profile1]proposal prop                      --指定安全提
议
[AR1-ipsec-profile-profile1]ike-peer toshanghai                --指定IKE对
等实体
[AR1-ipsec-profile-profile1]quit

[AR1]interface Tunnel 0/0/0                                    --定义到上海
网络的隧道接口
[AR1-Tunnel0/0/0]ip address 172.16.0.1 24                      --指定隧道接
口的地址
[AR1-Tunnel0/0/0]tunnel-protocol ?                             --查看隧道可
以使用的协议
  gre         Generic Routing Encapsulation
  ipsec       IPSEC Encapsulation
  ipv4-ipv6   IP over IPv6 encapsulation
  ipv6-ipv4   IPv6 over IP encapsulation
  mpls        MPLS Encapsulation
  none        Null Encapsulation
[AR1-Tunnel0/0/0]tunnel-protocol ipsec                         --隧道协议使
用ipsec
[AR1-Tunnel0/0/0]source 20.1.1.1                               --定义隧道的
起点（源地址）
[AR1-Tunnel0/0/0]destination 20.1.2.1                          --定义隧道的
终点（目标地址）
[AR1-Tunnel0/0/0]ipsec profile profile1                        --绑定IPSec
框架
[AR1-Tunnel0/0/0]quit

[AR1]ip route-static 10.1.2.0 24 172.16.0.2                    --添加到上海
网络的路由
```

AR3上的配置如下。

```
[AR3]ipsec proposal prop                                    --创建安全提
议，名为prop
[AR3-ipsec-proposal-prop]quit                               --使用默认参
数

[AR3]ike peer tobeijing v2                                  --创建IKE对
等实体
[AR3-ike-peer-tobeijing]peer-id-type ip                     --选择IP地址
作为对等ID
[AR3-ike-peer-tobeijing]pre-shared-key simple 91xueit       --指定预共享
密钥
[AR3-ike-peer-tobeijing]quit

[AR3]ipsec profile profile1                                 --创建安全框
架
[AR3-ipsec-profile-profile1]proposal prop                   --指定安全提
议
[AR3-ipsec-profile-profile1]ike-peer tobeijing              --指定IKE对
等实体
[AR3-ipsec-profile-profile1]quit

[AR3]interface Tunnel 0/0/0                                 --定义到北京
网络的隧道接口
[AR3-Tunnel0/0/0]ip address 172.16.0.2 24                   --指定隧道接
口的地址
[AR3-Tunnel0/0/0]tunnel-protocol ipsec                      --隧道协议使
用ipsec
[AR3-Tunnel0/0/0]source 20.1.2.1                            --定义隧道的
起点（源地址）
[AR3-Tunnel0/0/0]destination 20.1.1.1                       --定义隧道的
终点（目标地址）
[AR3-Tunnel0/0/0]ipsec profile profile1                     --绑定IPSec
框架
[AR3-Tunnel0/0/0]quit

[AR3]ip route-static 10.1.1.0 24 172.16.0.1                --添加到北京网
络的路由
```

13.3 远程访问VPN

还有一种VPN是远程访问VPN，这种VPN用于在外出差的员工通过Internet访问企业内网。将企业路由器配置成VPN服务器，在外出差的员工将计算机接入Internet就可以建立到企业内网的VPN拨号连接，拨通之后就可以像在公司内网中一样访问网络资源。

如图13-13所示，AR1是企业路由器，将其配置为VPN服务器，从PC3建立到AR1的VPN拨号连接，VPN服务器分配给PC3内网地址192.168.18.4。注意：分配给远程计算机的IP地址位于一个独立的网段中。PC3访问PC2时，网络层先使用内网地址进行封装，我们称其为内网数据包，该数据包不能在Internet中传输；把内网数据包当作数据，使用VPN服务器的公网地址和PC3的公网地址再次被封装为公网数据包，公网数据包就能通过Internet到达VPN服务器了；VPN服务器再将公网封装的部分去掉，将内网数据包发送到企业内网。图13-13是PC3访问PC2时数据包在Internet和内网中的封装示意图，这里省去了数据包加密和完整性封装。

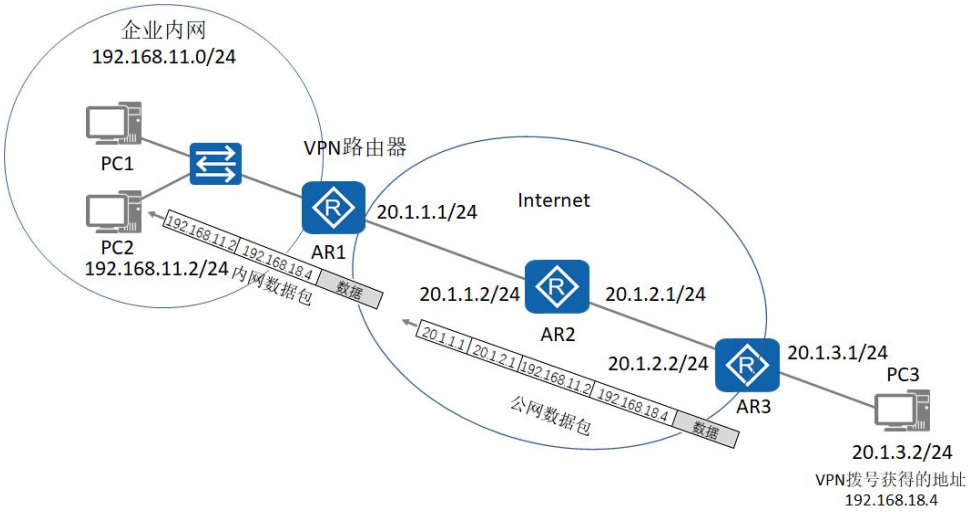


图13-13　远程访问VPN的网络拓扑

远程访问VPN使用的协议有L2TP、PPTP。L2TP是IETF标准协议，意味着各种设备厂商的设备之间用L2TP一般不会有问题；而PPTP是微软提出的，有些非微软的设备不一定支持。

将AR1配置成VPN服务器，需要完成以下配置。

（1）创建VPN拨号账号和密码。

（2）为VPN客户端创建一个地址池。

（3）配置虚拟接口模板。

（4）启用L2TP协议支持，创建L2TP组。

AR1的详细配置如下。

创建VPN拨号账号和密码。

```
[AR1]aaa
[AR1-aaa]local-user hanligang password cipher 91xueit
[AR1-aaa]local-user hanligang service-type ppp
[AR1-aaa]quit
```

为VPN客户端创建一个地址池。

```
[AR1]ip pool remotePool
[AR1-ip-pool-remotePool]network 192.168.18.0 mask 24
[AR1-ip-pool-remotePool]gateway-list 192.168.18.1
[AR1-ip-pool-remotePool]quit
```

配置虚拟接口模板。

```
[AR1]interface Virtual-Template 1
[AR1-Virtual-Template1]ip address 192.168.18.1 24  --设置接口地址
[AR1-Virtual-Template1]ppp authentication-mode pap --PPP身份验证模式
[AR1-Virtual-Template1]remote address pool remotePool --指定给远程计
算机分配地址的地址池
[AR1-Virtual-Template1]quit
```

启用L2TP协议支持，创建L2TP组。

```
[AR1]l2tp enable                                    --启用L2TP
[AR1]l2tp-group 1                                   --创建L2TP组
[AR1-l2tp1]tunnel authentication                    --启用隧道身份验证
[AR1-l2tp1]tunnel password simple huawei            --指定隧道身份验证
密钥
[AR1-l2tp1]allow l2tp virtual-template 1            --虚拟接口模板允许
使用L2TP
[AR1-l2tp1]quit
```

将VMWare Workstation中的Windows 10虚拟机充当图13-13中的PC3，在Windows 10中安装华为VPN客户端软件VPNClient_V100R001C02SPC702.exe。

安装完成后，运行该软件，出现新建连接向导，如图13-14所示，选中“通过输入参数创建连接”，单击“下一步”。



图13-14　选择创建方法

出现“第一步：输入登录设置”对话框，如图13-15所示，输入LNS服务器的地址、拨号账号和密码，单击“下一步”。



图13-15　输入登录设置

如图13-16所示，出现“第二步：请输入L2TP设置”对话框，选中“启用隧道验证功能”，输入隧道验证密码，单击“下一步”。

如图13-17所示，出现“最后一步：新建连接完成”对话框，输入连接的名称，单击“完成”。

VPN拨号成功后，在Windows 7虚拟机的命令提示符下输入ipconfig，查看拨号建立的连接和从VPN服务器获得的IP地址。



图13-16　输入L2TP设置



图13-17　完成新建连接

```
C:\Users\win7>ipconfig
Windows IP 配置

以太网适配器 本地连接* 12:                    --VPN拨号建立的连接

   连接特定的 DNS 后缀 .......:
   本地链接 IPv6 地址.........: fe80::99ea:c587:55ff:b385%23
   IPv4 地址 .............: 192.168.18.254
   子网掩码  .............: 255.255.255.0
   默认网关...............: 192.168.1.1

以太网适配器 本地连接 2:
   连接特定的 DNS 后缀 .......:
   本地链接 IPv6 地址.........: fe80::7c8a:eb3c:50b2:4cfe%17
   IPv4 地址 .............: 20.1.3.200
   子网掩码  .............: 255.255.255.0
   默认网关...............:
```

建立VPN拨号后，ping内网中的PC1和PC2，测试是否能够访问企业内网。如果不通，则需要关闭Windows 7中的防火墙。

13.4　习题

1．两台主机之间使用IPsec VPN传输数据，为了隐藏真实的IP地址，使用IPsec VPN的哪种封装较好？（　　）

A．AH

B．传输模式

C．隧道模式

D．ESP

2．如图13-18所示，两台私网主机之间希望通过GRE隧道进行通信。当GRE隧道建立之后，网络管理员需要在RTA上配置一条静态路由，将主机A访问主机B的流量引入隧道中，下列静态路由配置能满足要求的是（　　）。

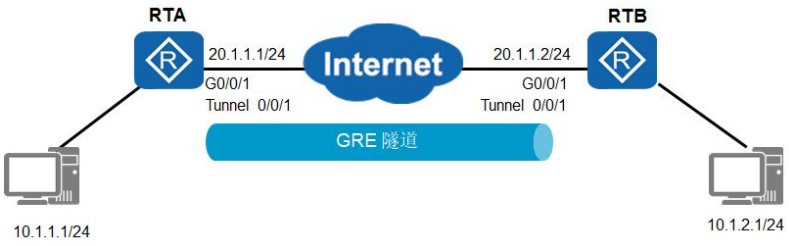


图13-18　通信示意

A．ip route-static 10.1.2.0 24 GigabitEthernet 0/0/1

B．ip route-static 10.1.2.0 24 200.2.2.1

C. ip route-static 10.1.2.0 24 200.1.1.1

D. ip route-static 10.1.0.24 tunnel 0/0/1

3. IP报文中的协议类型字段值为多少表示协议为GRE?

A. 47

B. 48

C. 2

D. 1

第14章　WLAN技术

本章内容

- WLAN概述
- WLAN的基本概念
- WLAN的工作原理
- WLAN的配置实现
- WLAN的技术发展趋势

以有线电缆或光纤作为传输介质的有线局域网应用广泛，但有线传输介质的铺设成本高、位置固定、移动性差。随着人们对网络的便携性和移动性的要求日益增强，传统的有线网络已经无法满足需求，无线局域网（Wireless Local Area Network，WLAN）技术应运而生。目前，WLAN已经成为一种经济、高效的网络接入方式。

本章介绍了WLAN在不同阶段的发展历程，其次介绍了WLAN技术相关的概念以及常见组网架构的工作原理，最后介绍WLAN常见组网架构的基本配置。

14.1 WLAN概述

14.1.1 什么是WLAN

WLAN即Wireless LAN（无线局域网），是指通过无线技术构建的无线局域网络。WLAN广义上是指以无线电波、激光、红外线等无线信号来替代有线局域网中的部分或全部传输介质所构成的网络。注意：这里指的无线技术不仅包含Wi-Fi，还有红外、蓝牙、ZigBee等。

通过WLAN技术，用户可以方便地接入无线网络，并在无线网络覆盖区域内自由移动，摆脱有线网络的束缚，如图14-1所示。

无线网络根据应用范围可分为WPAN、WLAN、WMAN、WWAN。

- WPAN (Wireless Personal Area Network)：个人无线网络，常用技术有Bluetooth、ZigBee、NFC、HomeRF、UWB。
- WLAN (Wireless Local Area Network)：无线局域网，常用技术有Wi-Fi。（WLAN中也会使用WPAN的相关技术。）
- WMAN (Wireless Metropolitan Area Network)：无线城域网，常用技术有WiMax。
- WWAN (Wireless Wide Area Network)：无线广域网，常用技术有GSM、CDMA、WCDMA、TD-SCDMA、LTE、5G。

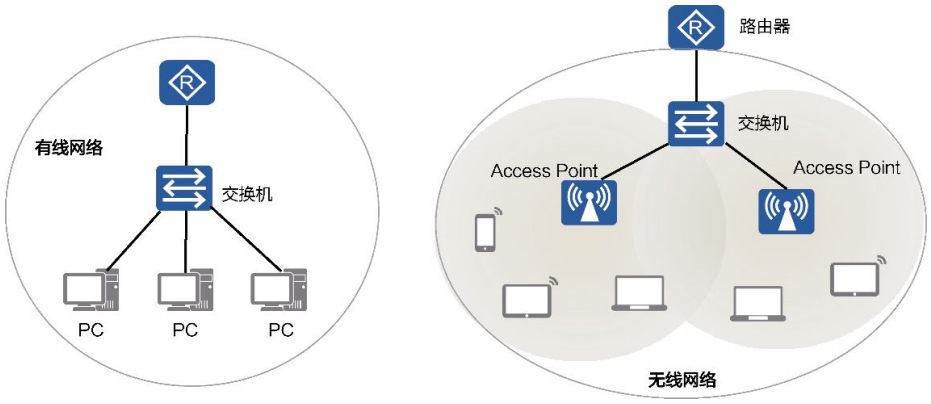


图14-1　有线网络和无线网络

WLAN相对于目前的有线宽带网络主要具备以下优点。

- 网络使用自由：凡是自由空间均可连接网络，不受限于线缆和端口位置。在办　公大楼、机场候机厅、度假村、商务酒店、体育场馆、咖啡店等场所WLAN尤为适用。
- 网络部署灵活：对于地铁、公路交通监控等难于布线的场所，采用WLAN进行无线网络覆盖，免去或减少了繁杂的网络布线，实施简单，成本低，扩展性好。

本章介绍的WLAN特指通过Wi-Fi技术基于802.11标准系列，利用高频信号（例如2.4GHz或5GHz）作为传输介质的无线局域网。

14.1.2　WLAN标准和Wi-Fi世代

IEEE 802.11是现今无线局域网的标准，它是由国际电机电子工程协会（IEEE）定义的无线网络通信的标准。

Wi-Fi联盟（全称国际Wi-Fi联盟组织，英语为Wi-Fi Alliance，简称WFA）是一个商业联盟，拥有 Wi-Fi的商标。它负责Wi-Fi 认证与商标授权的工作。联盟成立于1999年，主要目的是在全球范围内推行Wi-Fi产品的兼容认证，Wi-Fi是一种创建于IEEE 802.11标准上的无线局域网技术。在大多数场景下，Wi-Fi可等同于802.11。

图14-2标出了IEEE 802.11标准与Wi-Fi世代。

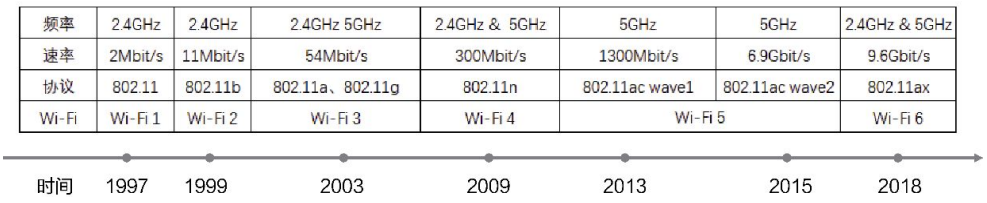


图14-2　IEEE 802.11标准和Wi-Fi世代

IEEE 802.11标准聚焦在TCP/IP对等模型的下两层。数据链路层主要负责信道接入、寻址、数据帧校验、错误检测、安全机制等内容。物理层主要负责在空口（空中接口）中传输比特流，规定所使用的频段等。

IEEE 802.11第一个版本发表于1997年。此后，更多的基于IEEE 802.11的补充标准逐渐被定义，最为熟知的是影响Wi-Fi代际演进的标准：802.11b、802.11a、802.11g、802.11n、802.11ac等。

在IEEE 802.11ax标准推出之际，Wi-Fi联盟将新Wi-Fi规格的名字简化为Wi-Fi 6，主流的IEEE 802.11ac改称Wi-Fi 5、IEEE 802.11n改称Wi-Fi 4，其他世代以此类推。

14.1.3 Wi-Fi在办公场景的发展趋势

Wi-Fi在办公场景下的发展趋势分为以下几个阶段。

第一阶段：初级移动办公时代，无线作为有线的补充。

WaveLAN技术的应用可以被认为是最早的企业WLAN雏形。早期的Wi-Fi技术主要应用在类似“无线收音机”这样的物联设备上，但是随着802.11a/b/g标准的推出，无线连接的优势越来越明显。企业和消费者开始认识到Wi-Fi技术的应用潜力，无线热点开始出现在咖啡店、机场和酒店。

Wi-Fi也在这一时期诞生，它是Wi-Fi联盟的商标，该联盟最初的目的是为了推动802.11b标准的制定，并在全球范围内推行Wi-Fi产品的兼容认证。随着标准的演进和遵从标准产品的普及，人们往往将Wi-Fi等同于802.11标准。

802.11标准是众多WLAN技术中的一种，只是802.11标准已成为业界的主流技术，所以人们提到WLAN时，通常是指使用Wi-Fi技术的WLAN。

这是WLAN应用的第一阶段，主要是解决“无线接入”的问题，核心价值是摆脱有线的束缚，设备在一定范围内可以自由移动，用无线网络延伸了有线网络。但是这一阶段的WLAN对安全、容量和漫游等方面没有明确的诉求，接入点（Access Point，AP）的形态还是单个接入点，用于单点组网覆盖。通常称单个接入点架构的AP为FAT AP。

第二阶段：无线办公时代，有线无线一体化。

随着无线设备的进一步普及，WLAN从起初仅仅作为有线网络的补充，发展到和有线网络一样不可或缺，由此进入第二阶段。

在这个阶段，WLAN作为网络的一部分，还需要为企业访客提供网络接入。

办公场景下存在大量视频、语音等大带宽业务，这对WLAN的带宽有更大的需求。从2012年开始，802.11ac标准趋于成熟，对工作频段、信道带宽、调制与编码方式等做出了诸多改进。与以往的Wi-Fi标准相比，它具有更高的吞吐率、更少的干扰，能够允许更多的用户接入。

第三阶段：全无线办公时代，以无线为中心。

目前，WLAN已经进入第三阶段，在办公环境中，无线网络基本彻底替代有线网络。办公区采用全Wi-Fi覆盖，有的办公位不再提供有线网口，办公环境更为开放和智能。

未来，云桌面办公、智真会议、4K视频等大带宽业务将从有线网络迁移至无线网络，而VR/AR等新技术将直接基于无线网络部署。新的应用场景对WLAN的设计与规划提出更高的要求。

2018年，新一代Wi-Fi标准Wi-Fi 6（IEEE命名为802.11ax，Wi-Fi 6是Wi-Fi联盟的命名）发布，这是Wi-Fi发展史上的又一重大里程碑。Wi-Fi 6的核心价值

是容量的进一步提升，引领无线通信进入10Gbit/s时代；多用户并发性能提升4倍，让网络在高密度接入、业务重载的情况下，依然保持优秀的服务能力。

14.2　WLAN基本概念和产品

14.2.1　WLAN设备介绍

华为无线局域网产品形态丰富，覆盖室内室外、家庭、企业等多种应用场景，可提供高速、安全和可靠的无线网络连接，如图14-3所示。

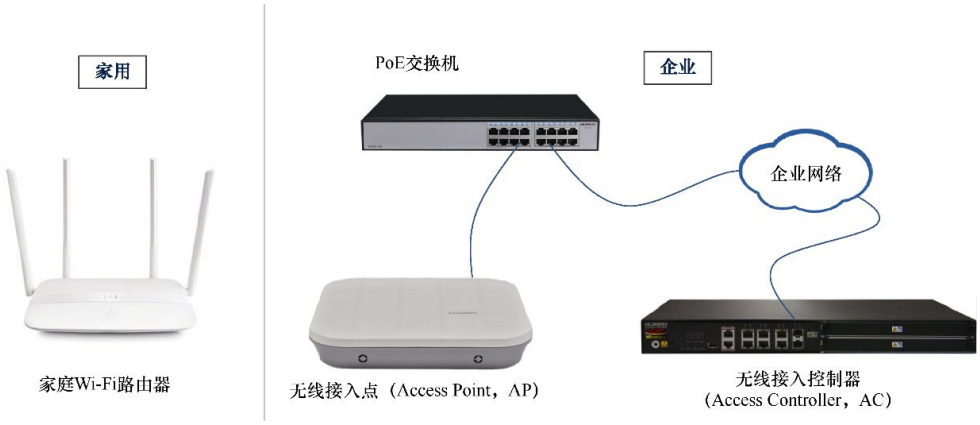


图14-3　家用无线设备和企业用无线设备

家庭WLAN产品有家庭Wi-Fi路由器，家庭Wi-Fi路由器通过把有线网络信号转换成无线信号，供计算机、手机等设备接收，从而实现无线上网功能。

企业WLAN产品包括AP、AC和PoE交换机。

- 无线接入点（Access Point，AP）。

AP有3种工作模式FAT AP（胖AP）、FIT AP（瘦AP）和云管理AP三种工作模式，根据网络规划的需求，用户可以灵活地在多种模式下切换。

FAT AP：适用于家庭，独立工作，需单独配置，功能较为单一，成本低。它可独立完成用户接入、认证、数据安全、业务转发和QoS等功能。

FIT AP：适用于大中型企业，需要配合AC使用。它由AC统一管理和配置，功能丰富，对网络维护人员的技能要求较高。用户接入、FIT AP的AP上线、认证、路由、AP管理、安全协议、QoS等功能需要同AC配合完成。

云管理：适用于中小型企业，需要配合云管理平台使用，由云管理平台统一管理和配置，功能丰富，即插即用，对网络维护人员的技能要求低。

- 无线接入控制器（Access Controller，AC）。

AC一般位于整个网络的汇聚层，可提供高速、安全、可靠的WLAN业务。AC能提供大容量、高性能、高可靠性、易安装、易维护的无线数据控制业务，具有组网灵活、绿色节能等优势。

- PoE交换机。

以太网供电（Power over Ethernet，PoE）是指通过以太网网络进行供电，也被称为基于局域网的供电系统（Power over LAN，PoL）或有源以太网（Active Ethernet）。PoE允许电功率通过传输数据的线路或空闲线路传输到终端设备。在WLAN网络中，可以通过PoE交换机对AP设备进行供电。

14.2.2　基本的WLAN组网架构

WLAN网络架构分有线侧和无线侧两部分，如图14-4所示，有线侧是指AP上行到Internet的网络，使用以太网协议。无线侧是指STA到AP之间的网络，使用802.11协议。

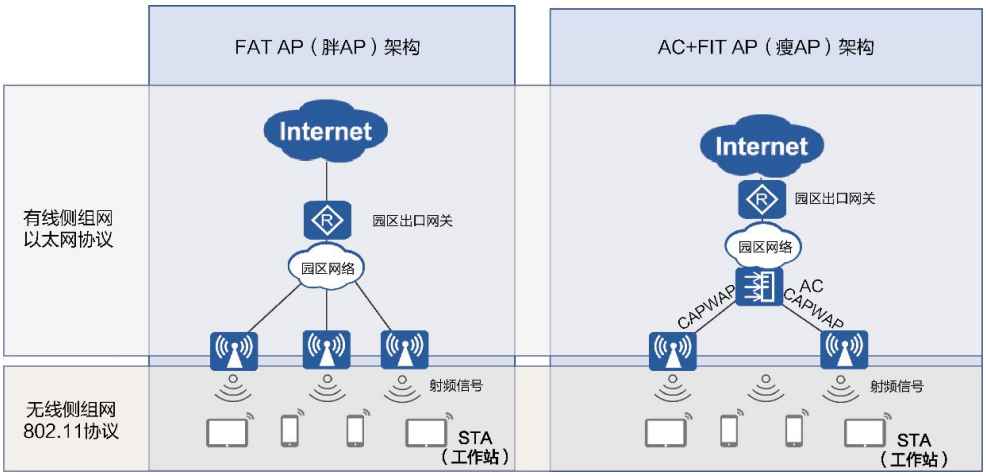


图14-4　WLAN组网架构

无线侧接入的WLAN网络架构为集中式架构。它从最初的FAT AP架构，演进为AC+FIT AP架构。

- FAT AP（胖AP）架构。

这种架构不需要专门的设备集中控制就可以完成无线用户的接入、业务数据的加密和业务数据报文的转发等功能，因此又称为自治式网络架构。

适用范围：家庭。

特点：AP独立工作，需要单独配置，功能较为单一，成本低。

缺点：随着WLAN覆盖面积增大，接入用户的增多，需要部署的FAT AP数量也会增多，但FAT AP是独立工作的，缺少统一的控制设备，因此管理维护这些FAT AP就十分麻烦。

- AC+FIT AP（瘦AP)架构。

在这种架构中，AC负责WLAN的接入控制、转发和统计、AP的配置监控、漫游管理、AP的网管代理、安全控制；FIT AP负责802.11报文的加解密、802.11的物理层功能、接受AC的管理等简单功能。

适用范围：大中型企业。

特点：AP需要配合AC使用，由AC统一管理和配置，功能丰富，对网络运维人员的技能要求高。

注意：在本章中，我们主要以AC+FIT AP架构为例进行讲解。

WLAN的基本概念如下。

- 工作站STA（Station）：支持802.11标准的终端设备，例如，带无线网卡的计算机、支持WLAN的手机等。
- 无线接入控制器（Access Controller，AC）：在AC+FIT AP网络架构中，AC对无线局域网中的所有FIT AP进行控制和管理。例如，AC可以通过与认证服务器交互信息来为WLAN用户提供认证服务。
- 无线接入点（Access Point，AP）：为STA提供基于802.11标准的无线接入服务，起到有线网络和无线网络的桥接作用。
- 无线接入点控制与规范（Control And Provisioning of Wireless Access Points，CAPWAP）：由RFC5415协议定义的，实现AP和AC之间的互通的一个通用封装和传输机制。
- 射频信号（无线电磁波）：提供基于802.11标准的WLAN技术的传输介质，是具有远距离传输能力的高频电磁波。本章中的射频信号是2.4G或5G频段的无线电磁波。

14.2.3 敏捷分布式AP架构

在过去5年时间里，Wi-Fi网络的接入终端数量增加了10倍，承载的数据流量增加了4倍，且70%的数据传输发生在室内。虽然近些年WLAN新产品和新协议不断推陈出新，然而室内弱覆盖问题一直没有得到妥善解决，主要原因是传统放装方案信号在穿墙之后会形成盲区。在房间数量较多的大型酒店或者高等学校宿舍部署时，需要部署数千个的AP，增加了管理上的难度。

要从根本上解决这个问题，无线网络架构的变革是关键。华为推出的敏捷分布式Wi-Fi解决方案，将传统AC+Fit AP架构的二级架构变革为AC+中心AP+远端射频单元的三级分布式架构。其中，中心AP统一处理业务、配置和漫游功能，实现性能的提升和管理节点的节省；同时，分布式架构将射频单元通过网线送入房间，实现无死角的信号覆盖，将每房间的用户容量从32个提升至80个，每用户带宽从10Mbit/s提升至20Mbit/s；而且，射频单元只负责无线接入和数据转发，相对于传统放装AP，性能提升20%。

敏捷分布式AP（以下简称敏分AP）架构通过分布式覆盖解决酒店或宿舍的多房间信号覆盖问题和大量AP带来的管理问题，如图14-5所示。

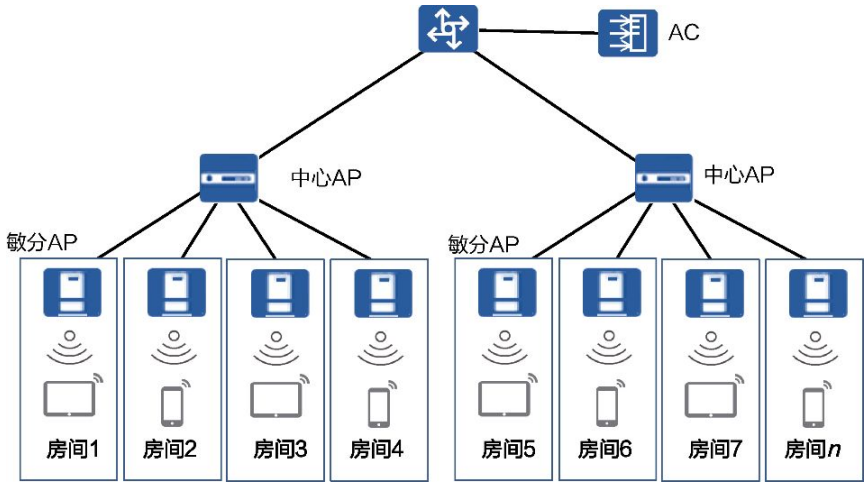


图14-5　敏捷分布式AP架构

14.2.4　有线侧组网概念

有线侧组网涉及的概念有CAPWAP、AP-AC组网方式和AC连接方式。

1. CAPWAP

为满足大规模组网的要求，且需要对网络中的多个AP进行统一管理，IETF成立了无线接入点控制和配置协议（Control And Provisioning of Wireless

Access Points Protocol，CAPWAP）工作组，最终制定CAPWAP。该协议定义了AC如何对AP进行管理、业务配置，即AC与AP间首先会建立CAPWAP隧道，然后AC通过CAPWAP隧道来实现对AP的集中管理和控制，如图14-6所示。

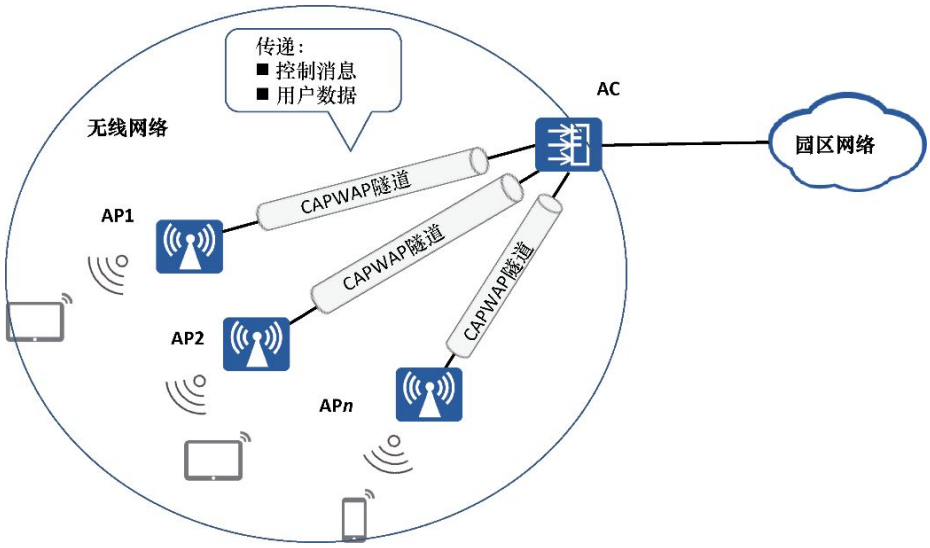


图14-6　CAPWAP隧道

CAPWAP隧道功能如下所列。

- AP与AC之间的状态维护。
- AC通过CAPWAP隧道对AP进行管理和业务配置下发。
- 当采用隧道模式转发时，AP通过CAPWAP隧道实现STA发出的数据与AC之间的交互。

CAPWAP是基于UDP进行传输的应用层协议。CAPWAP在传输层运输两种类型的消息。

- 业务数据流量，封装转发无线数据帧。
- 管理流量，管理AP和AC之间交换的管理消息。

CAPWAP数据和控制报文基于不同的UDP端口发送。管理流量端口为UDP端口5246，业务数据流量端口为UDP端口5247。

2. AP-AC组网方式

AP和AC间的组网分为二层组网和三层组网，如图14-7所示。

二层组网是指AP和AC之间的网络为直连或者二层网络。二层组网AP可以通过二层广播或者DHCP过程来实现AP即插即用上线。二层组网比较简单，适用于简单临时的组网，能够进行比较快速的组网配置，但不适用于大型组网架构。

三层组网指的是AP与AC之间的网络为三层网络。 AP无法直接发现AC，需要通过DHCP或DNS方式动态发现，也可通过配置静态IP发现。在实际组网中，一台AC可以连接几十甚至几百台AP，组网情况一般比较复杂。比如在企业网络中，AP可以放在办公室，会议室，会客间等场所，而AC可以安放在公司机房。这样，AP和AC之间的网络就是比较复杂的三层网络。因此，在大型组网中一般采用三层组网。

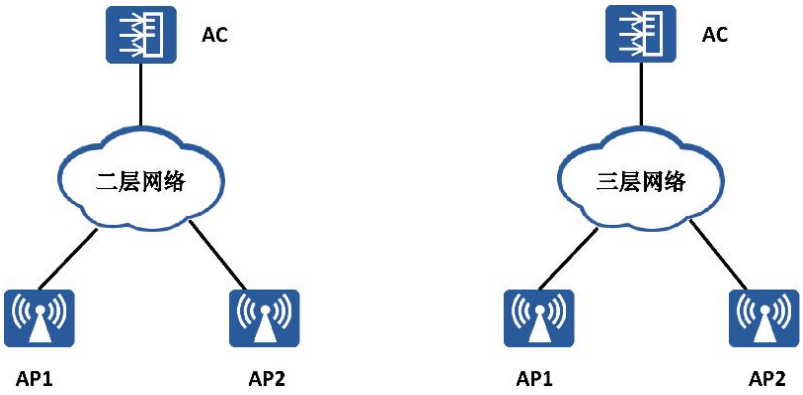


图14-7　AP-AC组网方式

3. AC连接方式

AC的连接方式分为直连式组网和旁挂式组网，如图14-8所示。

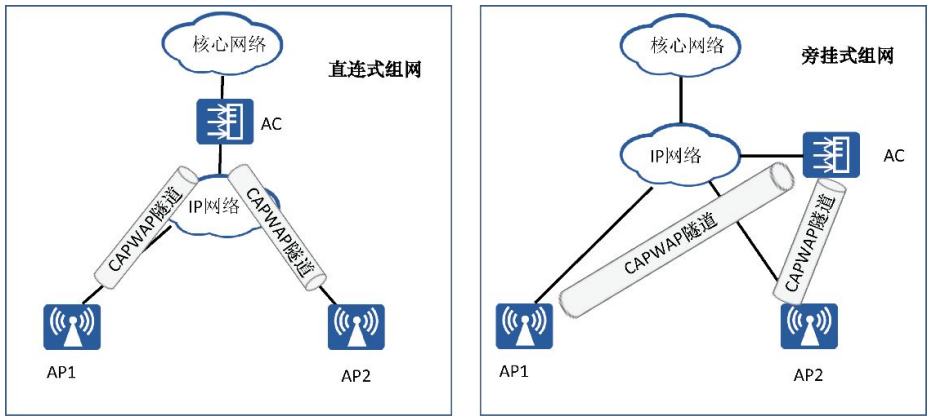


图14-8　AC连接方式

直连式组网AC部署在用户的转发路径上。在直连模式下用户流量要经过AC，会消耗AC的转发能力，对AC的吞吐量以及处理数据的能力要求比较高。如果AC性能差，那它有可能是整个无线网络带宽的瓶颈。但用此种组网，组网架构清晰，组网实施起来简单。

旁挂式组网AC旁挂在AP与上行网络的直连网络中，不直接连接AP。AP的业务数据可以不经过AC而直接到达上行网络。

由于在实际组网中，大部分不是早期就规划好无线网络，无线网络的覆盖架设是后期在现有网络中扩展而来。而采用旁挂式组网就比较容易进行扩展，只需将AC旁挂在现有网络中，比如旁挂在汇聚交换机上，就可以对终端AP进行管理。所以此种组网方式使用率比较高。

在旁挂式组网中，AC只承载对AP的管理功能，管理流封装在CAPWAP隧道中传输。数据业务流可以通过CAPWAP隧道经AC转发，也可以不经过AC转发直接转发，后者无线用户业务流经汇聚交换机由汇聚交换机传输至上层网络。

14.2.5　无线侧组网概念

1. 无线通信系统

在无线通信系统中，信息可以是图像、文字、声音等。如图14-9所示，信息需要先经过信源编码转换为方便电路计算机处理的数字信号，再经过信道编码和调制，转换为无线电波发射出去。接收端收到后经过解调、解码得到信息。

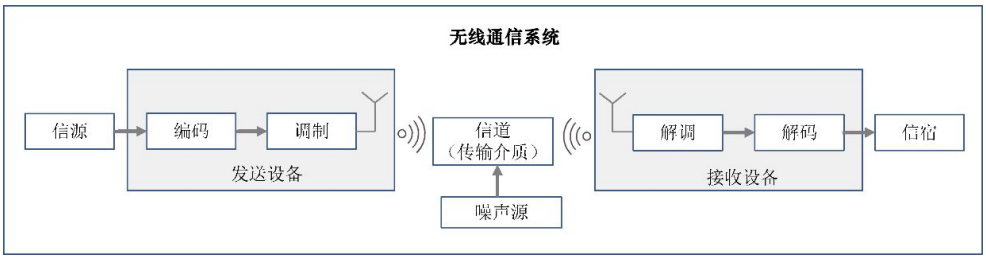


图14-9　无线通信系统

下面介绍无线通信涉及的一些概念。

- 信源编码：将最原始的信息经过对应的编码转换为数字信号的过程。
- 信道编码：是一种对信息纠错、检错的技术，可以提升信道传输的可靠性。信息在无线传输过程中容易受到噪声的干扰，导致接收信息出错，引入信道编码能够在接收设备上最大限度地恢复信息、降低误码率。
- 调制：数字信号叠加到高频振荡电路产生的高频信号上，才能通过天线转换成无线电波发射出去。叠加动作就是调制的过程。
- 信道：传输信息的通道，无线信道就是空间中的无线电波。
- 空中接口：简称空口，无线信道使用的接口。发送设备和接收设备使用空口和信道连接，对于无线通信，空口是不可见的，连接着不可见的空间。

2. 无线电磁波

无线电磁波是频率介于3Hz和300GHz之间的电磁波，也叫作射频电波，简称射频、射电，如图14-10所示。无线电技术将转换后的声音讯号或其他信号利用无线电磁波传播。

WLAN技术就是通过无线电磁波在空间传输信息。当前WLAN技术使用的频段是：

- 2.4GHz频段（2.4GHz～2.4835GHz）；
- 5GHz频段（5.15GHz～5.35GHz，5.725GHz～5.85GHz）。

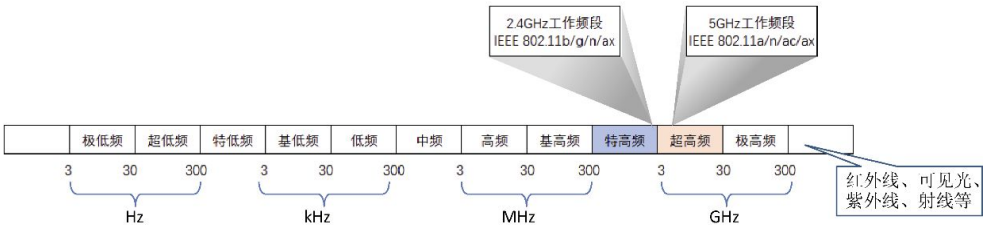


图14-10　无线电磁波频谱

极低频（3Hz～30Hz）：潜艇通信或直接转换成声音。

超低频（30Hz～300Hz）：直接转换成声音或交流输电系统（50～60Hz）。

特低频（300Hz～3kHz）：矿场通信或直接转换成声音。

甚低频（3kHz～30kHz）：直接转换成声音、超声，常见于地球物理学研究。

低频（30kHz～300kHz）：国际广播。

中频（300kHz～3MHz）：用于调幅（AM）广播、海事及航空通信。

高频（3MHz～30MHz）：短波，用于民用电台。

甚高频（30MHz～300MHz）：用于调频（FM）广播、电视广播、航空通信。

特高频（300MHz～3GHz）：用于电视广播、无线电话通信、无线网络、微波炉。

超高频（3GHz～30GHz）：用于无线网络、雷达、人造卫星接收。

极高频（30GHz～300GHz）：用于射电天文学、遥感、人体扫描安检仪。

300GHz以上：红外线、可见光、紫外线、射线等。

3. 无线信道

信道是传输信息的通道，无线信道就是空间中的无线电磁波。无线电磁波无处不在，如果随意使用频谱资源，那将带来无穷无尽的干扰问题，所以无线通信协议除了要定义允许使用的频段，还要精确划分频率范围，每个频率范围就是信道。

无线网络（路由器、AP热点、计算机无线网卡）可在多个信道上运行。在无线信号覆盖范围内的各种无线网络设备应该尽量使用不同的信道，以避免信号之间的干扰。

图14-11展示了 2.4GHz（=2400MHz）频带的信道划分。实际一共有14个信道（图14-11画出了第14信道），但第14信道一般不用。图14-11只列出信道的中心频率。每个信道的有效宽度是 20MHz，另外还有2MHz的强制隔离频带（类似于公路上的隔离带）。例如，对于中心频率为 2412 MHz 的1信道，其频率范围为2401～2423MHz。

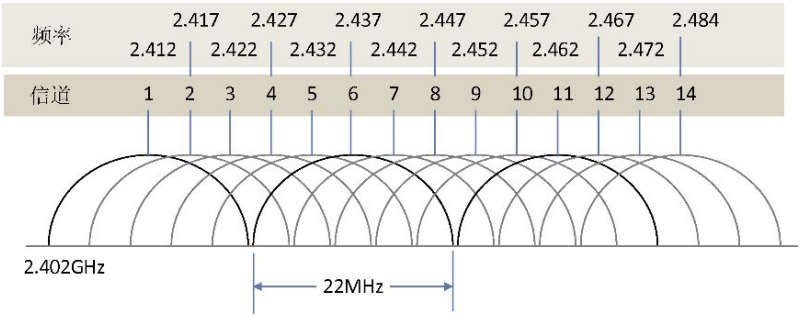


图14-11　2.4GHz信道划分

目前主流的无线Wi-Fi网络设备不管是802.11b/g还是802.11b/g/n 一般都支持13个信道。它们的中心频率虽然不同，但是因为都占据一定的频率范围，所以会有一些相互重叠的情况。图14-11展示了这13个信道的频率范围列表。了解这

13个信道所处的频段，有助于我们理解人们经常说的三个不互相重叠的信道含义。

从图14-11很容易看到其中 1、6、11 这三个信道（深颜色标记）之间是完全没有交叠的，也就是人们常说的三个不互相重叠的信道。每个信道 20MHz 带宽。从图14-11也很容易看清楚其他各信道之间频谱重叠的情况。另外，除 1、6、11 三个一组互不干扰的信道，还有 2、7、12；3、8、13；4、9、14 三组互不干扰的信道。

在WLAN中，AP的工作状态会受到周围环境的影响。例如，当相邻AP的工作信道存在重叠频段时，某个AP的功率过大会对相邻AP造成信号干扰。

通过射频调优功能，动态调整AP的信道和功率，可以使同一AC管理的各AP的信道和功率保持相对平衡，保证AP工作在最佳状态。

4. BSS/SSID/BSSID

基本服务集（Basic Service Set，BSS）是一个AP覆盖的范围，是无线网络的基本服务单元，通常由一个AP和若干STA组成。BSS是802.11网络的基本结构，如图14-12所示。由于无线介质共享性，BSS中的报文收发需携带BSSID（MAC地址）。

终端要发现和找到AP，需要通过AP的一个身份标识，这个身份标识就是基本服务集标识符（Basic Service Set Identifier，BSSID）。BSSID是AP上的数据链路层MAC地址。为了区分BSS，要求每个BSS都有唯一的BSSID，因此使用AP的MAC地址来保证其唯一性。

如果一个空间部署了多个BSS，终端就会发现多个BSSID，只要选择加入的BSSID就行。但是做选择的是用户，为了使得AP的身份更容易辨识，则用一个字

符串来作为AP的名字。这个字符串就是服务集标识符（Service Set Identifier，SSID），需使用SSID代替BSSID。

SSID是无线网络的标识，用来区分不同的无线网络，AP可以发送SSID以便于无线设备选择和接入。例如，当我们在便携式计算机上搜索可接入无线网络时，显示出来的网络名称就是SSID，如图14-13所示。

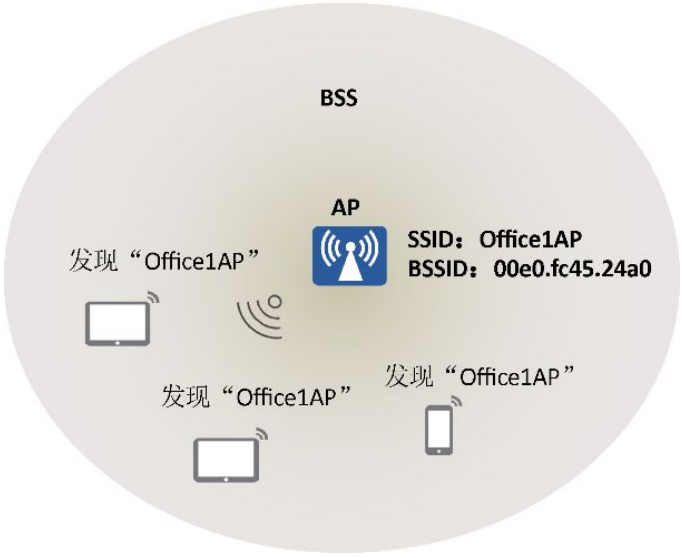


图14-12　BSS



图14-13　发现的SSID

5. VAP

早起的AP只支持1个BSS，如果要在同一个空间中部署多个BSS，则需要安放多个AP，这不但增加了成本，还占用了信道资源。为了改善这种情况，现在的AP通常支持创建多个虚拟AP（Virtual Access Point，VAP）。

虚拟接入点VAP是在一个物理实体AP上虚拟出多个AP。每个被虚拟出来的AP就是一个VAP。每个VAP提供和物理实体AP一样的功能。如图14-14所示，每个VAP对应一个BSS，这样1个AP就可以提供多个BSS，可以再为这些BSS设置不同的SSID和不同的接入密码。这样可以为不同的用户群体提供不同的无线接入服务，比如

通过VAP1接入无线网络的计算机不允许访问Internet，通过VAP2接入无线网络的计算机允许访问Internet。

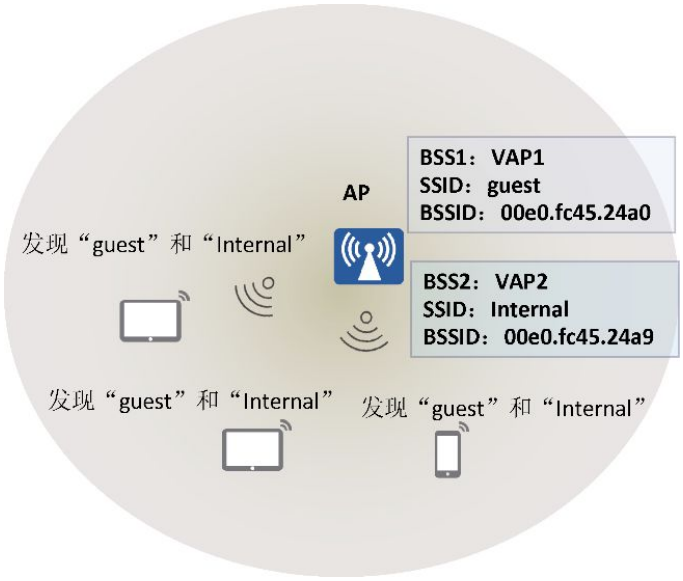


图14-14　VAP

VAP简化了WLAN的部署，但不意味VAP越多越好，要根据实际需求进行规划。一味增加VAP的数量，不仅要让用户花费更多的时间找到SSID，还会增加AP配置的复杂度。而且VAP并不等同于真正的AP，所有的VAP都共享这个AP的软件和硬件资源，所有VAP的用户都共享相同的信道资源，所以AP的容量是不变的，并不会随着VAP数目的增加而成倍地增加。

6. ESS

为了满足实际业务的需求，需要对BSS的覆盖范围进行扩展。同时用户从一个BSS移动到另一个BSS时，不能感知到SSID的变化，则可以通过扩展服务集（Extend Service Set，ESS）来实现，如图14-15所示。

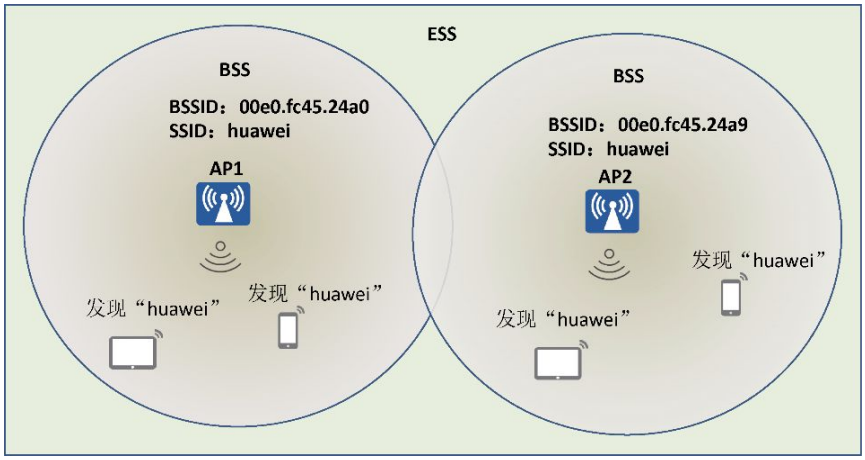


图14-15　扩展服务集

ESS是由采用相同的SSID的多个BSS组成的更大规模的虚拟BSS。用户可以带着终端在ESS内自由移动和漫游，不管用户移动到哪里，都可以认为使用的同一个WLAN。

STA在同属一个ESS的不同AP的覆盖范围之间移动且保持用户业务不中断的行为，我们称之为WLAN漫游。

WLAN网络的最大优势就是STA不受物理介质的影响，可以在WLAN覆盖范围内四处移动并且能够保持业务不中断。同一个ESS内包含多个AP设备，当STA从一个AP覆盖区域移动到另外一个AP覆盖区域时，利用WLAN漫游技术可以实现STA用户业务的平滑切换。

14.3　WLAN的工作原理

14.3.1　WLAN工作流程

在AC+FIT AP组网架构中，计算机是通过AC对AP进行统一的管理，因此所有的配置都是在AC上进行的。WLAN的工作流程分为4个阶段，如图14-16所示。

1．AP上线，AP获取IP地址并发现AC，然后与AC建立连接。

2．AC将WLAN业务配置下发到AP生效。

3．STA搜索AP发送的SSID并连接，然后上线接入网络。

4．WLAN网络开始转发业务数据。

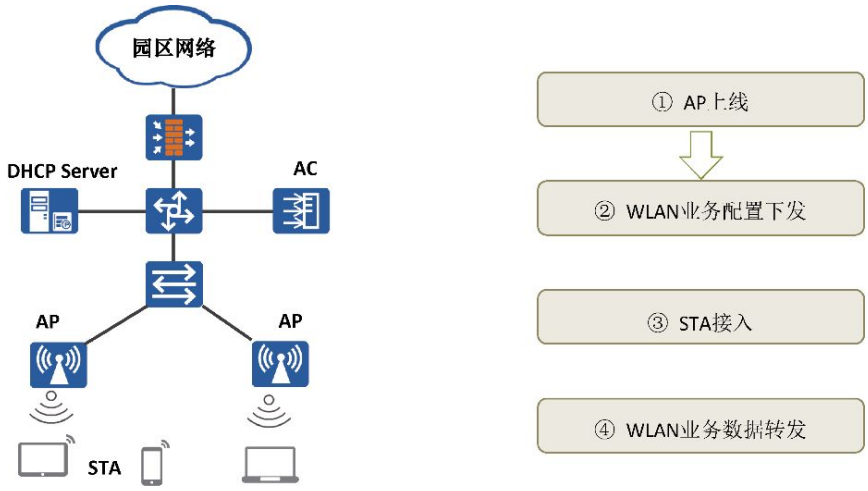


图14-16　WLAN工作流程

14.3.2　第一阶段：AP上线

FIT AP需完成上线过程，AC才能实现对AP的集中管理和控制，以及业务下发。AP的上线过程包括以下步骤：

1．在AC的预配置；

2．AP获取IP地址；

3．AP发现AC并与之建立CAPWAP隧道；

4．AP接入控制；

5．AP版本升级；

6．CAPWAP隧道维持。

步骤1：在AC预配置

为确保AP能够上线，AC需要预先配置如下内容。

- 配置网络互通：配置DHCP服务器，为AP和STA分配IP地址，也可以将AC设备配置为DHCP服务器。配置AP与DHCP服务器之间的网络互通，配置AP与AC之间的网络互通。
- 创建AP组：每个AP都会加入并且只能加入到一个AP组中，AP组通常用于多个AP的通用配置。
- 配置AC的国家码（域管理模板）：域管理模板提供对AP的国家码、调优信道集合和调优带宽等的配置。国家码用来标识AP频射所在的国家，不同国家码规定了不同的AP频射特性，包括AP的发送功率、支持的信道等。配置国家码是为了使AP的射频特性符合不同国家或区域的法律法规要求。
- 配置源接口或源地址（与AP建立隧道）：每台AC都必须唯一指定一个IP地址、VLANIF接口或者Loopback接口，该AC设备下挂接的AP学习到此IP地址或者此接口下配置的IP地址，以用于AC和AP间的通信。此IP地址或者接口称为源地址或源接口。只有为每台AC指定唯一一个源接口或源地址，AP才能与AC建立CAPWAP隧道。设备支持使用VLANIF接口或Loopback接口作为源接口，支持使用VLANIF接口或Loopback接口下的IP地址作为源地址。
- 配置AP上线时自动升级（可选）：自动升级是指AP在上线过程中自动对比自身版本与在AC、SFTP或FTP服务器上配置的AP版本是否一致，如果不一致，则进行升级，然后AP自动重启再重新上线。

- 添加AP设备（配置AP认证模式）：即配置AP认证模式，AP上线。添加AP有三种方式：离线导入AP、自动发现AP以及手动确认未认证列表中的AP。

步骤2：AP获取IP地址

AP必须获得IP地址才能够与AC通信，然后WLAN网络才能够正常工作。AP获取IP地址有两种方式，一种方式是静态方式，需要登录到AP设备上手动配置IP地址。另一种方式是DHCP方式，通过配置DHCP服务器，使AP作为DHCP客户端向DHCP服务器请求IP地址。

可以部署Windows服务器或Linux服务器作为专门的DHCP服务器为AP分配IP地址。也可以使用AC的DHCP服务为AP分配IP地址，还可以使用网络中的设备，比如三层交换或路由器为AP分配IP地址。

步骤3：AP发现AC并与之建立CAPWAP隧道

AP通过发送Discovery Request报文可找到可用的AC。AP发现AC有两种方式。

第一种是静态方式，AP预先配置AC的静态地址列表。当AP上线时，如图14-17所示，AP发送Discovery Request单播报文到所有预配置列表对应IP地址的AC。然后AP接收AC返回的Discovery Response报文，并选择一个AC开始建立CAPWAP隧道。

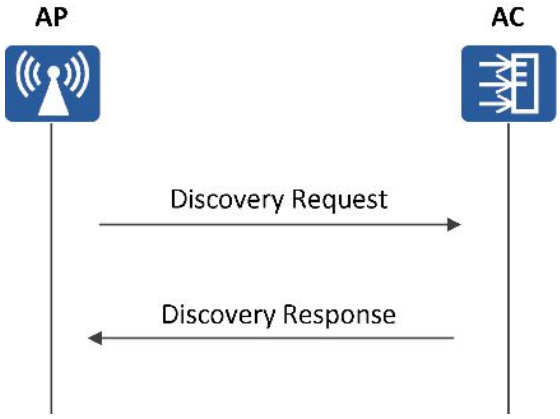


图14-17 AP返回CA

第二种是动态方式，动态方式又分为DHCP方式、DNS方式和广播方式。本章主要介绍DHCP方式和广播方式。

DHCP方式发现AC的过程如下。

AP要想通过配置DHCP服务器发现AC，那么DHCP响应报文中必须携带Option 43，且Option 43携带AC的IP地址列表。DHCP的option 43选项是告诉APAC的IP地址，让AP寻找AC进行注册。

华为设备，如交换机、路由器、AC等，作为DHCP服务器时要配置Option 43选项。

以IP地址为192.168.22.1的AC为例，HDCP服务器配置命令为option 43 sub-option 3 hex 3139322E3136382E32322E31或者option 43 sub-option 3 ascii 192.168.22.1。

其中，sub-option 3为固定值，代表子选项类型；hex 3139322E3136382E32322E31与ascii 192.168.22.1分别是AC地址192.168.22.1的HEX（十六进制）格式和ASCII格式。

对于涉及多个AC、Option要填写多个IP地址的情形，IP地址同样要以“，”间隔，逗号“，”对应的ASCII值为2C。比如两个AC的IP地址分别为192.168.22.1和192.168.22.2，则DHCP服务器上的配置命令为option 43 sub-option 3 hex 3139322E3136382E3130302E322 C3139322E3136382E3130302E33或option 43 sub-option 3 ascii 192.168.22.1,192.168.22.2。

AP通过DHCP服务获取AC的IP地址后，使用AC发现机制来获知哪些AC是可用的，决定与最佳AC建立CAPWAP的连接。

AP启动CAPWAP的发现机制，以单播或广播的形式发送发现请求报文以试图关联AC。AC收到AP的Discovery Request以后，会给AP发送一个单播Discovery Response，AP可以通过Discover Response中所含有的AC优先级或者AC上当前AP的个数等，确定与哪个AC建立会话。

广播方式发现AC的过程如下。

当AP启动后，如果DHCP方式和DNS方式均未获得AC的IP或AP发出发现请求报文后未收到响应，则AP启动广播发现流程，以广播的方式发出发现请求报文。

接收到发现请求报文的AC检查该AP是否有接入本机的权限（已经授权的MAC地址或者序列号），如果有则发回响应。如果该AP没有接入权限，AC则拒绝请求。

广播发现方式只适用于AC/AP间为二层可达的网络场景。

AP发现AC后会完成CAPWAP隧道的建立。CAPWAP隧道包括数据隧道和控制隧道，用来维护AP与AC之间的状态。

数据隧道用于把AP接收的业务数据报文经过CAPWAP数据隧道集中到AC上转发，同时还可以选择对数据隧道进行数据传输层安全（Datagram Transport Layer Security，DTLS）加密。启用DTLS加密功能后，CAPWAP数据报文都会经过DTLS加解密。

控制隧道用于AP与AC之间的管理报文的交换。我们还可以选择对控制隧道进行数据传输层安全加密，启用DTLS加密功能后，CAPWAP控制报文都会经过DTLS加解密。

步骤4：AP接入控制

AP发现AC后，会发送Join Request报文。AC收到AP发送的Join Request报文之后，会进行AP合法性认证，认证通过则添加相应的AP设备，并响应Join Response报文，如图14-18所示。

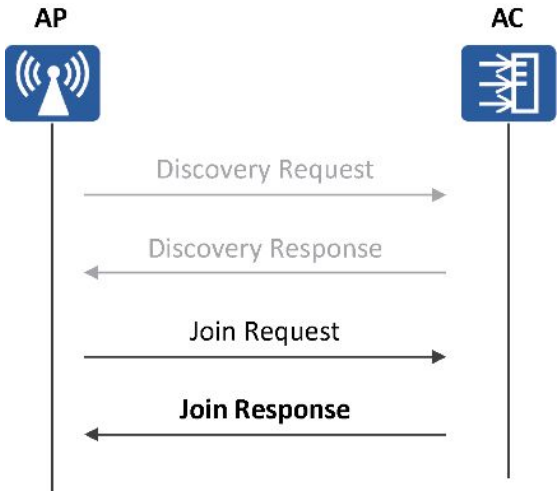


图14-18 AP加入AC

AC支持三种对AP的认证方式：

- MAC认证；
- 序列号（SN）认证；
- 不认证。

在AC上添加AP的方式有以下三种。

- 离线导入AP：预先配置AP的MAC地址和SN，当AP与AC连接时，如果AC发现AP和预先配置的AP的MAC地址和SN匹配，则AC开始与AP建立连接。
- 自动发现AP：若配置AP的认证模式为不认证，或配置AP的认证模式为MAC或SN认证且将AP加入AP白名单中，则当AP与AC连接时，AP将被AC自动发现并正常上线。
- 手动确认未认证列表中的AP：当配置AP的认证模式为MAC或SN认证，但AP没有离线导入且不在已设置的AP白名单中，则该AP会被记录到未授权的AP列表中。需要用户手动确认后，此AP才能正常上线。

步骤5：AP的版本升级

如图14-19所示，AP根据收到的Join Response报文中的参数判断当前的系统软件版本是否与AC指定的一致。如果不一致，则AP通过发送Image data Request报文请求软件版本，然后进行版本升级。升级方式包括AC模式、FTP模式集合（即SFTP模式）。AP在软件版本更新完成后重启，再重复进行前面的步骤2、3、4。

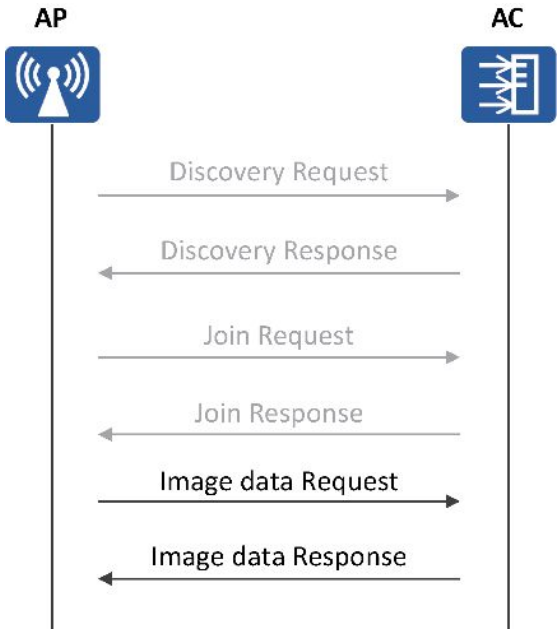


图14-19 版本升级请求和响应

AC上AP升级的方式分为自动升级和定时升级。

自动升级：主要用于AP还未在AC中上线的场景。通常先配置好AP上线时的自动升级参数，然后再配置AP接入。AP在之后的上线过程中会自动完成升级。如果AP已经上线，那么在配置完自动升级参数后，以任意方式触发AP重启，AP也会进行自动升级。相比于自动升级，使用在线升级方式升级能够减少业务中断的时间。升级方式的三种模式介绍如下。

- AC模式：AP升级时从AC上下载升级版本，适用于AP数量较少的场景。
- FTP模式：AP升级时从FTP服务器上下载升级版本，适用于网络安全性要求不是很高的文件传输场景。此方法采用明文传输数据，存在安全隐患。

- SFTP模式：AP升级时从SFTP服务器上下载升级版本，适用于网络安全性要求高的场景。该方法对传输数据进行了严格加密和完整性保护在线升级：主要用于AP已经在AC中上线并已承载了WLAN业务的场景。

定时升级主要用于AP已经在AC中上线并已承载了WLAN业务的场景。通常指定在网络访问量少的时间段升级。

步骤6：CAPWAP隧道维持

数据隧道维持通过AP与AC之间交互Keepalive （UDP端口号为5247）报文来检测数据隧道的连通状态。

控制隧道维持通过AP与AC交互Echo（UDP端口号为5246）报文来检测控制隧道的连通状态。

14.3.3 第二阶段：WLAN业务配置下发

AC向AP发送Configuration Update Request请求消息，AP回应Configuration Update Response消息，AC再将AP的业务配置信息下发给AP，如图14-20所示。

AP上线后，会主动向AC发送Configuration Status Request报文，该报文中包含了现有AP的配置。当AP的当前配置与AC的要求不符合时，AC会通过Configuration Status Response通知AP。

说明：AP上线后，首先会主动向AC获取当前配置，而后统一由AC对AP进行集中管理和业务配置下发。

1. 配置模板

WLAN网络中存在着大量的AP，为了简化AP的配置操作步骤，可以将AP加入AP组中，在AP组中统一对AP进行同样的配置。但是每个AP也有着不同于其他AP的参数配置，不便通过AP组来进行统一配置，这类个性化的参数可以直接在每个AP下配置。每个AP在上线时都会加入并且只能加入一个AP组中。当AP从AC上获取到AP组和AP个性化的配置后，会优先使用AP的配置。

AP组和AP都能够引用如下模板，域管理模板、射频模板、VAP模板，如图14-21所示。部分模板还能继续引用其他模板，这些模板统称为WLAN模板。

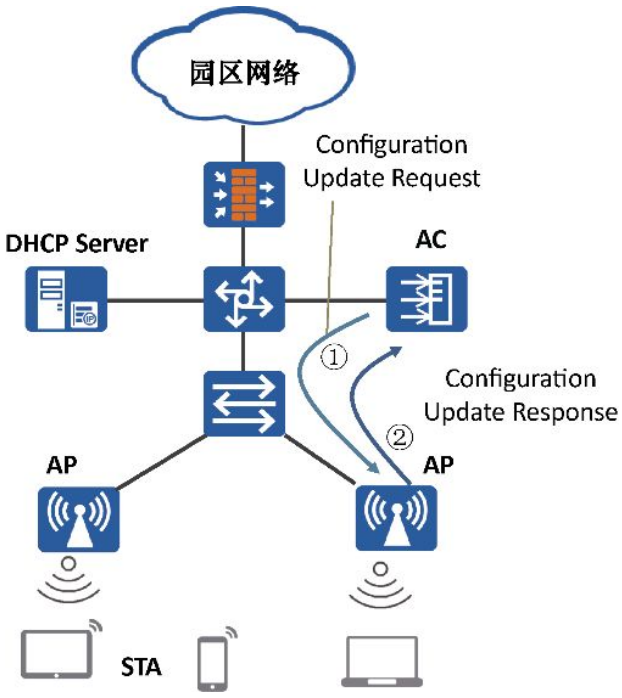


图14-20　配置升级请求和响应

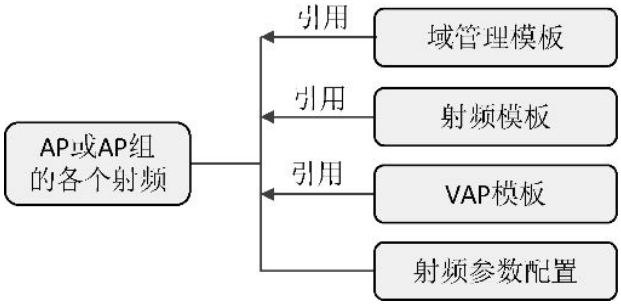


图14-21　AP或AP组引用的模板

- 域管理模板。

国家码用于标识AP射频所在的国家，不同国家码规定了不同的AP射频特性，包括AP的发送功率、支持的信道等。配置国家码是为了使AP的射频特性符合不同国家或区域的法律法规要求。

通过配置调优信道集合，用户可以在配置射频调优功能时指定AP信道动态调整的范围，同时避开雷达信道和终端不支持信道。

- 射频模板。

根据实际的网络环境对射频的各项参数进行调整和优化，使AP具备满足实际需求的射频能力，从而提高WLAN网络的信号质量。射频模板中各项参数下发到AP后，只有AP支持的参数才会在AP上生效。

该模板可配置的参数包括：射频的类型、射频的速率、射频的无线报文组播发送速率、AP发送Beacon帧的周期等。

- VAP模板。

在VAP模板下配置各项参数，然后在AP组或AP中引用VAP模板，AP就会生成VAP，VAP用来为STA提供无线接入服务。通过配置VAP模板下的参数，使AP实现为STA提供不同无线业务服务的能力。

VAP模板还能继续引用SSID模板、安全模板、流量模板等。

- 射频参数配置。

AP射频需要根据实际的WLAN网络环境来配置不同的基本射频参数，以使AP射频的性能达到更优。

在WLAN网络中，相邻AP的工作信道存在重叠频段时，容易产生信号干扰，这对AP的工作状态会产生影响。为避免信号干扰，使AP工作在最佳状态，提高WLAN

网络质量，可以手动配置相邻AP工作在非重叠信道上。

根据实际网络环境的需求来配置射频的发射功率和天线增益，使射频信号强度满足实际网络需求，从而提高WLAN网络的信号质量。

在实际应用场景中，两个AP之间的距离可能为几十米到几十千米，因为AP间的距离不同，所以AP之间传输数据时等待ACK报文的时间也不相同。通过调整合适的超时时间参数，可以提高AP间的数据传输效率。

2. VAP模板

VAP模板要引用SSID模板、安全模板，还可以配置数据转发方式和业务VLAN，如图14-22所示。

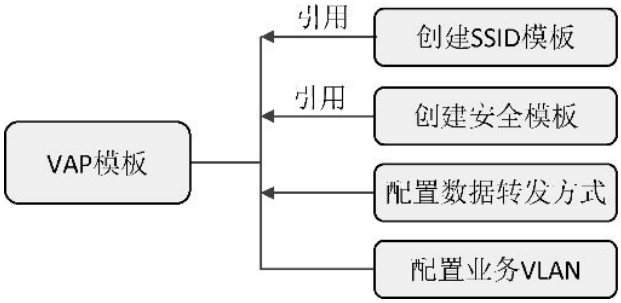


图14-22 VAP需要配置的参数和引用的模板

- SSID模板。

SSID模板主要用于配置WLAN网络的SSID名称，还可以配置其他功能，主要包括如下功能。

- 隐藏SSID功能：用户在创建无线网络时，为了保护无线网络的安全，可以对无线网络名称进行隐藏设置。这样，只有知道网络名称的无线用户才能连接到这个无线网络中。
- 单个VAP下能够关联成功的最大用户数：单个VAP下接入的用户数越多，每个用户能够使用的平均网络资源就越少。为了保证用户的上网体验，可以根据实际的网络状况来配置合理的最大用户接入数。
- 用户数达到最大时自动隐藏SSID的功能：使能用户数达到最大时自动隐藏SSID的功能后，当WLAN网络下接入的用户数达到最大时，SSID会被隐藏，新用户将无法搜索到SSID。

- 安全模板。

配置WLAN安全策略后，AP可以对无线终端进行身份验证，对用户的报文进行加密，从而保护WLAN网络和用户的安全。

WLAN安全策略支持开放认证、WEP、WPA/WPA2-PSK、WPA/WPA2-802.1X等，在安全模板中选择其中一种进行配置即可。

- 数据转发方式。

控制报文是通过CAPWAP的控制隧道转发的，用户的数据报文分为隧道转发（又称为“集中转发”）方式和直接转发（又称为“本地转发”）方式。这部分内容在后面会详细介绍。

- 业务VLAN。

由于WLAN无线网络灵活的接入方式，STA可能会在某个地点（例如办公区入口或体育场馆入口）集中接入同一个WLAN无线网络中，然后漫游到其他AP覆盖的无线网络环境下。

业务VLAN被配置为单个VLAN时，在接入STA数众多的区域中容易出现IP地址资源不足、而其他区域IP地址资源浪费的情况。

业务VLAN被配置为VLAN pool时，可以在VLAN pool中加入多个VLAN，然后通过将VLAN pool配置为VAP的业务VLAN，实现一个SSID能够同时支持多个业务VLAN的目的。新接入的STA会被动态地分配到VLAN pool中的各个VLAN中，减少了单个VLAN下的STA数目，缩小了广播域；同时每个VLAN尽量均匀地分配IP地址，减少了IP地址的浪费。

14.3.4 第三阶段：STA接入

CAPVAP隧道建立完成后，用户就可以接入无线网络。STA接入过程分为6个阶段：扫描阶段、链路认证阶段、关联阶段、接入认证阶段、STA地址分配（DHCP）、用户认证。

1. 扫描阶段

STA可以通过主动扫描来定期搜索周围的无线网络，以获取周围的无线网络信息。根据探测请求帧（Probe Request帧）是否携带SSID，可以将主动扫描分为两种，如图14-23所示。

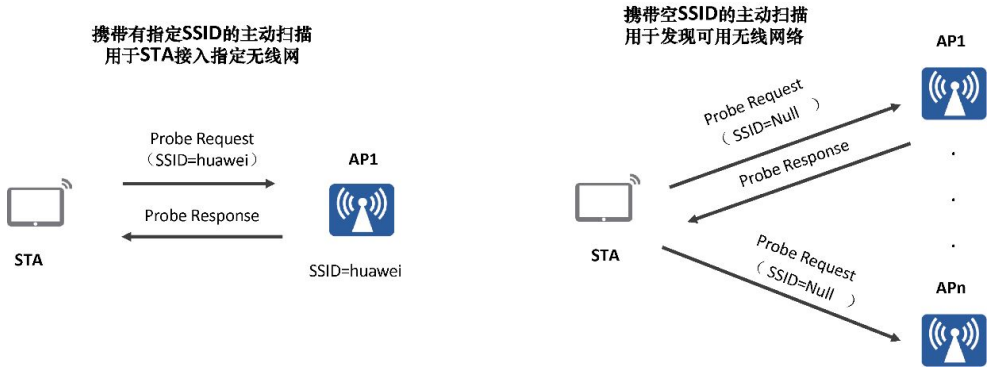


图14-23　主动扫描

携带有指定SSID的主动扫描方式适用于STA通过主动扫描接入指定的无线网络。客户端发送携带指定SSID的Probe Request，STA依次在每个信道发出Probe request帧，寻找与STA有相同SSID的AP。只有能够提供指定SSID无线服务的AP接收到该探测请求后才回复探查响应。

携带空SSID的主动扫描方式适用于STA通过主动扫描可以获知是否存在可使用的无线服务。客户端发送广播Probe Request，客户端会定期地在其支持的信息列表中发送Probe Request帧扫描无线网络。当AP收到Probe Request帧后，会回应Probe Response帧通告可以提供的无线网络信息。

STA也支持被动扫描搜索无线网络。被动扫描是指客户端通过侦听AP定期发送的Beacon帧（信标帧，包含SSID、支持速率等信息）来发现周围的无线网络。默认状态下AP发送Beacon帧的周期为100Tus（1TU=1024us）。

2. 链路认证阶段

WLAN技术是以无线射频信号作为业务数据的传输介质，这种开放的信道使得攻击者很容易对无线信道中传输的业务数据进行窃听和篡改，因此，安全性成为阻碍WLAN技术发展的重要因素之一。

WLAN安全提供了WEP（Wired Equivalent Privacy）、WPA、WPA2 (Wi-Fi Protected Access)等安全策略机制。每种安全策略都有一整套安全机制，包括无线链路建立时的链路认证方式，无线用户上线时的用户接入认证方式和无线用户传输数据业务时的数据加密方式。

为了保证无线链路的安全，接入过程AP需要完成对STA的认证。802.11链路定义了两种认证机制：开放系统认证和共享密钥认证。

开放系统认证即不认证，任意STA都可以认证成功。

共享密钥认证即STA和AP预先配置相同的共享密钥，然后验证两边的密钥配置是否相同，如果一致，则认证成功；否则，认证失败。

3. 关联阶段

完成链路认证后，STA会继续发起链路服务协商，具体的协商通过Association报文实现。终端关联过程实质上就是链路服务协商的过程，协商内容包括支持的速率、信道等。

4. 接入认证阶段

接入认证即对用户进行区分，并在用户访问网络之前限制其访问权限。相对于链路认证，接入认证的安全性更高。接入认证主要包含PSK认证和802.1X认证。

5. STA地址分配

STA获取自身的IP地址，是STA正常上线的前提条件。如果STA通过DHCP获取IP地址，那么可以将AC设备或汇聚交换机作为DHCP服务器来为STA分配IP地址。一般情况下使用汇聚交换机作为DHCP服务器。

6. 用户认证

用户认证是一种“端到端”的安全结构，包括802.1X认证、MAC认证和Portal认证。Portal认证也称Web认证，一般将Portal认证网站称为门户网站。用户上网时，必须在门户网站进行认证，只有认证通过后才可以使用网络资源。这个认证通常需要微信登录或手机短信来验证用户身份，因为微信或手机都是实名认证过的，这样就能记录接入网络的用户的信息，如果出现安全事件，可以追查到具体的人。

14.3.5 第四阶段：WLAN业务数据转发

CAPWAP中的数据包括控制报文（管理报文）和数据报文。控制报文通过CAPWAP的控制隧道转发。用户的数据报文分为隧道转发（又称为“集中转发”）方式和直接转发（又称为“本地转发”）方式。

隧道转发方式是指用户的数据报文到达AP后，需要经过CAPWAP数据隧道封装后发送给AC，然后AC再转发到上层网络。直接转发方式是指用户的数据报文到达AP后，不经过CAPWAP的隧道封装而直接转发给上层网络，如图14-24所示。

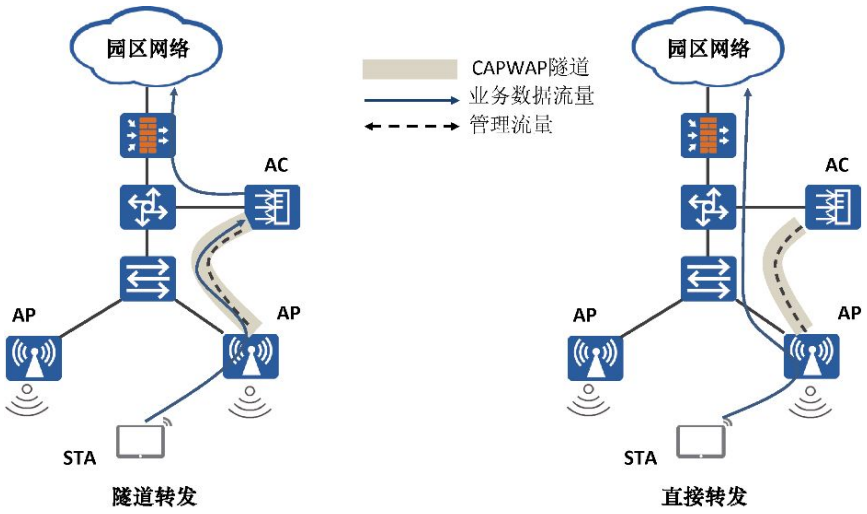


图14-24　隧道转发和直接转发

隧道转发方式的优点就是AC集中转发数据报文，安全性好，方便集中管理和控制；缺点是业务数据必须经过AC转发，报文转发效率比直接转发方式的效率低，AC受到的压力大。

直接转发方式的优点是数据报文不需要经过AC转发，报文转发效率高，AC所受压力小；缺点是业务数据不便于集中管理和控制。

14.4　案例：旁挂二层组网隧道转发

业务需求：企业用户通过WLAN接入网络，以满足移动办公的最基本需求。

组网需求具体如下。

- AC组网方式：旁挂二层组网。
- DHCP部署方式：AC作为DHCP服务器为AP和STA分配IP地址。

业务数据转发方式：隧道转发。

图 14-25 画出了本案例的物理拓扑和逻辑拓扑，由于是隧道转发，两个办公室的业务VLAN数据通过CAPWAP隧道发送到AC，因此就相当于在AC上连接了两个VLAN。AC和AP之间的通信使用管理VLAN 100。为了让大家更容易理解各个设备承担的角色，图12-24右侧展示了逻辑拓扑。

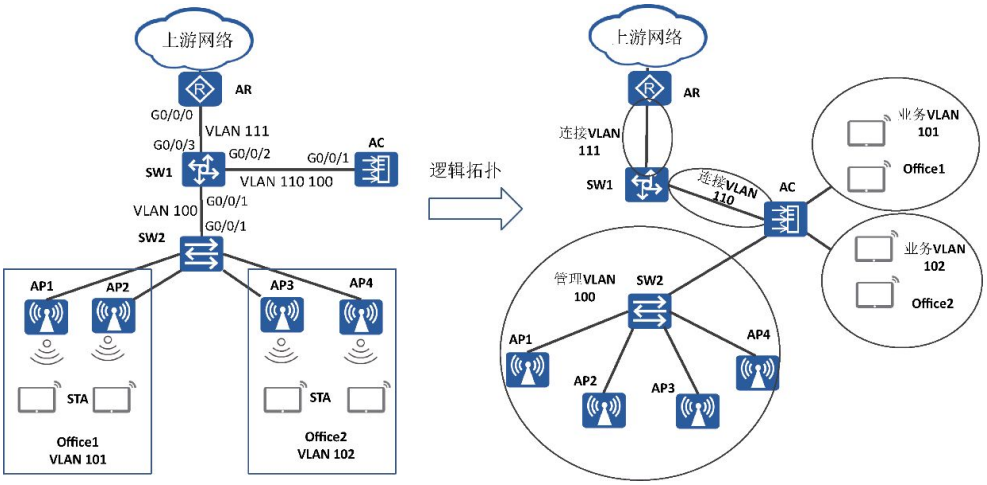


图14-25　物理拓扑和逻辑拓扑

可以看出，AC相当于一个路由器连接着VLAN 100、VLAN 101和VLAN 102，为了让这3个VLAN能够访问上游网络，还需要在AC和SW1上创建一个VLAN 110。创建该VLAN是为了连接AC和SW1，因此该VLAN称为互联VLAN。要想让SW1和上游路由器AR连接，我们需要创建一个VLAN 111。通过图12-25右侧的逻辑拓扑，各个设备

如何添加路由的思路就清晰了。SW1和SW2之间的连接只需要传送VLAN 100的帧，因此将SW1的GE0/0/1接口配置成Access接口，并指定到VLAN 100即可。SW1和AC之间的连接需要VLAN 110和VLAN 100的帧，因此需要配置成Trunk。

地址规划和模板配置如表14-1和表14-2所示。

表14-1　地址规划

数据	配置
AP管理VLAN	VLAN 100
Office1业务VLAN	VLAN 101
Office2业务VLAN	VLAN 102
SW1和AC互联VLAN	VLAN 110
SW1和RA互联VLAN	VLAN 111
VLAN 100网段	192.168.100.0/24
VLAN 101网段	192.168.101.0/24
VLAN 102网段	192.168.102.0/24
VLAN 110网段	192.168.110.0/24
VLAN 111网段	192.168.111.0/24

数据	配置
DHCP服务器	AC作为DHCP服务器为AP和STA分配地址
AC的源接口IP地址	VLANIF100:192.168.100.1/24

表14-2　模板配置

AP组	名称：ap-Office1 引用VAP模板：VAP-Office1 引用域管理模板：default
	名称：ap-Office2 引用VAP模板：VAP-Office2 引用域管理模板：default
域管理模板	名称：default 国家码：中国
SSID模板	名称：SSID-Office1 SSID名称：AP-Office1
	名称：SSID-Office2 SSID名称：AP-Office2
安全模板	名称：Sec-Office1 安全策略：WPA-WPA2+PSK 密码：a1234567
	名称：Sec-Office2 安全策略：WPA-WPA2+PSK 密码：b1234567
VAP模板	名称：VAP-Office1 转发模式：隧道转发 业务VLAN：VLAN 101 引用SSID模板：SSID-Office1 引用安全模板：Sec-Office1
	名称：VAP-Office2 转发模式：隧道转发 业务VLAN：VLAN 102 引用SSID模板：SSID-Office2 引用安全模板：Sec-Office2

配置WLAN的思路如下。

（1）配置AP、AC和周边网络设备之间实现网络互通。

（2）配置AP上线。

（3）创建AP组。将需要进行相同配置的AP都加入AP组，以实现统一配置。

（4）配置AC的系统参数，包括国家及地区码、AC与AP之间通信的源接口等。

（5）配置AP上线的认证方式并离线导入AP，以实现AP正常上线。

（6）配置WLAN业务参数，实现STA访问WLAN网络功能。

14.4.1　配置网络互通

在配置WLAN之前，先要配置AP、AC和周边网络设备之间实现网络互通。图14-26展示了本实验的逻辑拓扑，接口地址参照图14-26规划的地址进行设置。在AR路由器和SW1上添加路由，确保网络畅通。

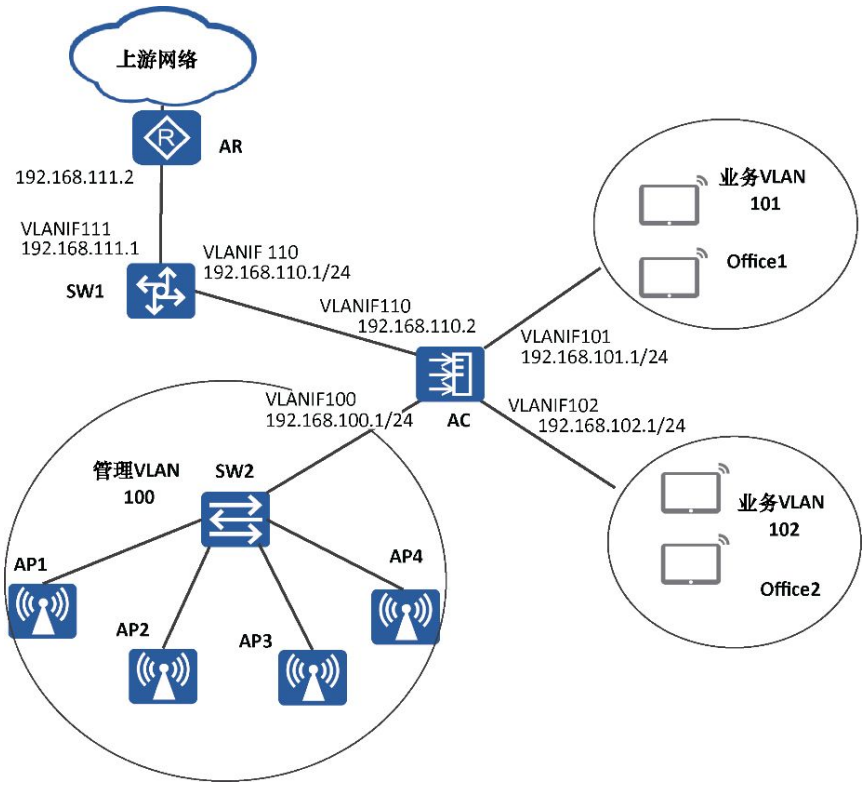


图14-26　逻辑拓扑

在AC上创建VLAN 100、VLAN 101、VLAN 102、VLAN 110。为VLANIF接口配置地址，以充当这些网段的网关，同时添加一条默认路由指向SW1的VLANIF110接口地址。在SW1上添加到VLAN 100、101、102网段的路由，下一跳指向AC的VLANIF110接口的地址。

在AC上配置DHCP服务，为VLAN 100、VLAN 101和VLAN 102分配地址。

在AR上的配置如下。

```
[AR]interface GigabitEthernet 0/0/0
[AR-GigabitEthernet0/0/0]ip address 192.168.111.2 24
[AR-GigabitEthernet0/0/0]quit
[AR]ip route-static 192.168.0.0 16 192.168.111.1
```

在SW1上的配置如下。

```
[SW1]vlan batch 100 110 111
[SW1]interface Vlanif 111
[SW1-Vlanif111]ip address 192.168.111.1 24
[SW1-Vlanif111]quit
[SW1]interface Vlanif 110
[SW1-Vlanif110]ip address 192.168.110.1 24
[SW1-Vlanif110]quit
[SW1]interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3]port link-type access
[SW1-GigabitEthernet0/0/3]port default vlan 111
[SW1-GigabitEthernet0/0/3]quit
[SW1]interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2]port link-type trunk
[SW1-GigabitEthernet0/0/2]port trunk allow-pass vlan 110 100
[SW1-GigabitEthernet0/0/2]quit
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]port link-type access
[SW1-GigabitEthernet0/0/1]port default vlan 100
[SW1-GigabitEthernet0/0/1]quit
[SW1]ip route-static 192.168.100.0 24 192.168.110.2
[SW1]ip route-static 192.168.101.0 24 192.168.110.2
[SW1]ip route-static 192.168.102.0 24 192.168.110.2
```

在AC上的配置如下。

```
[AC]vlan batch 100 101 102 110
[AC]interface Vlanif 100
[AC-Vlanif100]ip address 192.168.100.1 24
```

```
[AC-Vlanif100]interface Vlanif 101
[AC-Vlanif101]ip address 192.168.101.1 24
[AC-Vlanif101]interface Vlanif 102
[AC-Vlanif102]ip address 192.168.102.1 24
[AC-Vlanif102]interface Vlanif 110
[AC-Vlanif110]ip address 192.168.110.2 24
[AC]interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1]port link-type trunk
[AC-GigabitEthernet0/0/1]port trunk allow-pass vlan 110 100
[AC]ip route-static 0.0.0.0 0 192.168.110.1
```

DHCP服务的配置如下。

```
[AC]dhcp enable
[AC]interface Vlanif 100
[AC-Vlanif100]dhcp select interface
[AC-Vlanif100]interface Vlanif 101
[AC-Vlanif101]dhcp select interface
[AC-Vlanif101]interface Vlanif 102
[AC-Vlanif102]dhcp select interface
```

在AP输入display ip interface brief可以显示自动获得的IP地址。

```
[Huawei]display ip interface brief
Interface                   IP Address/Mask      Physical   Protocol
Vlanif1                     192.168.100.123/24   up         up
```

14.4.2 配置AP上线

在AC上创建域管理模板，然后创建AP组。在AP组中应用域管理模板，并配置AC的接口或源地址，然后将指定AP加入到AP组。

创建域管理模板。由于所有与WLAN相关的配置都需要在WLAN视图中完成，因此管理员需要首先通过wlan命令进入WLAN视图。

在WLAN视图下使用命令regulatory-domain-profile name *profile-name*来创建域管理模板，并进入该模板视图。在域管理模板中，管理员可以设置国家及地区码、优化信道和带宽等参数。以下操作可创建域管理模板default，指定国家及地区码为cn。

```
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name default
[AC-wlan-regulate-domain-default]country-code cn
[AC-wlan-regulate-domain-default]quit
[AC-wlan-view]
```

接着使用WLAN视图命令ap-group name group-name来创建名为ap-Office1和ap-Office2的AP组，同时进入了AP组的配置视图，在这里应用域管理模板。在更改AP组中应用的域管理模板时，系统会提示警告信息并要求管理员进行确认。如果管理员确认更改，那么输入y后按回车键，更改生效。

```
[AC-wlan-view]ap-group name ap-Office1
[AC-wlan-ap-group-ap-Office1]regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna
gain configurations of the radio and reset the AP. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-Office1]quit
[AC-wlan-view]ap-group name ap-Office2
[AC-wlan-ap-group-ap-Office2]regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna
gain configurations of the radio and reset the AP. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-Office2]quit
```

配置AC的源接口，使AP和AC的Vlanif 100接口的地址建立capwap隧道。

```
[AC]capwap source interface Vlanif 100
```

在AC上离线导入AP。下面的配置将AP加入到AP组中，以MAC地址认证的方式添加AP。

```
[AC-wlan-view]ap auth-mode ?            --查看支持的身份验证模式
      mac-auth  MAC authenticated mode, default authenticated mode
      no-auth   No authenticated mode
      sn-auth   SN authenticated mode
[AC-wlan-view]ap auth-mode mac-auth     --指定使用MAC地址身份验证
[AC-wlan-view]ap-id 1 ap-mac 00e0-fcc4-15a0
[AC-wlan-ap-1]ap-name ap1
[AC-wlan-ap-1]ap-group ap-Office1
Warning: This operation may cause AP reset. If the country code changes, it
will clear channel, power and antenna gain configurations of the radio,
Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-1]quit
[AC-wlan-view]ap-id 2 ap-mac 00e0-fcb1-02b0
[AC-wlan-ap-2]ap-name ap2
[AC-wlan-ap-2]ap-group ap-Office1
Warning: This operation may cause AP reset. If the country code changes, it
will clear channel, power and antenna gain configurations of the radio,
```

```
Whether to continue? [Y/N]:y
[AC-wlan-ap-2]quit
[AC-wlan-view]ap-id 3 ap-mac 00e0-fc33-5190
[AC-wlan-ap-3]ap-name ap3
[AC-wlan-ap-3]ap-group ap-Office2
Warning: This operation may cause AP reset. If the country code changes, it
will clear channel, power and antenna gain configurations of the radio,
Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-3]quit
[AC-wlan-view]ap-id 4 ap-mac 00e0-fcaf-5610
[AC-wlan-ap-4]ap-name ap4
[AC-wlan-ap-4]ap-group ap-Office2
Warning: This operation may cause AP reset. If the country code changes, it
will clear channel, power and antenna gain configurations of the radio,
Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-4]quit
```

将AP上线后，在AC上执行命令display ap all查看AP状态，看到AP的“State”字段为“nor”时，表示AP已经在AC成功上线，状态为正常。

```
[AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal          [4]
--------------------------------------------------------------------------------
ID   MAC        Name Group    IP         Type       State  STA    Up time
--------------------------------------------------------------------------------
1    00e0-fcc4-15a0 ap1  ap-Office1 192.168.100.123   AP2050DN    nor   0
14M:48S
2    00e0-fcb1-02b0 ap2  ap-Office1 192.168.100.20    AP2050DN    nor   0
12M:4S
3    00e0-fc33-5190 ap3  ap-Office2 192.168.100.11    AP2050DN    nor   0
10M:5S
4    00e0-fcaf-5610 ap4  ap-Office2 192.168.100.144   AP2050DN    nor   0
20S
--------------------------------------------------------------------------------
Total: 4
```

display ap命令的输出信息具体如下。

- ID：AP ID。
- MAC：AP MAC地址。
- Name：AP名称。
- Group：AP所属的AP组名称。

- IP：AP的IP地址。在NAT场景下，AP在私网侧，AC在公网侧，该值为AP私网侧的IP地址。
- Type：AP类型。
- State：AP状态。
- normal：AP为正常状态，指AP在AC上成功上线。
- commit-failed：AP上线后在WLAN业务配置下为失败状态。
- download：AP正在升级状态。
- fault：AP为上线失败状态。
- idle：AP和AC建立连接前的初始状态。
- STA：AP上接入的终端用户数。
- Uptime：AP已上线时长。
- ExtraInfo：额外的信息，P表示设备供电不足。

14.4.3 配置WLAN业务参数

管理员需要在AC上配置与WLAN相关的业务参数，包括SSID模板、安全模板和VAP模板。

（1）配置SSID模板。

由于两个办公室的SSID不一样，所以需要创建两个SSID模板。

```
[AC-wlan-view]ssid-profile name ssid-Office1
[AC-wlan-ssid-prof-ssid-Office1]ssid AP-Office1
[AC-wlan-ssid-prof-ssid-Office1]quit
[AC-wlan-view]ssid-profile name ssid-Office2
[AC-wlan-ssid-prof-ssid-Office1]ssid AP-Office2
[AC-wlan-ssid-prof-ssid-Office1]quit
```

管理员先使用命令wlan进入了WLAN视图，接着通过命令ssid-profile name *profile-name*创建了名为ssid-office1的SSID模板，并进入了该SSID模板的配置视图。SSID模板名称的长度为1～35字符，不区分大小写。在SSID模板中，管理员还可以配置其他参数，比如与QoS（服务质量）相关的参数。

（2）配置安全模板。

两个办公室连接AP的密码不一样，因此需要创建两个安全模板。

```
[AC-wlan-view]security-profile name Sec-Office1
[AC-wlan-sec-prof-Sec-Offce1]security wpa-wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-Sec-Offce1]quit
[AC-wlan-view]security-profile name Sec-Office2
[AC-wlan-sec-prof-Sec-Offce2]security wpa-wpa2 psk pass-phrase b1234567 aes
[AC-wlan-sec-prof-Sec-Offce2]quit
```

在本例中，管理员在AC上创建了Sec-Office1和Sec-Office2两个安全模板。安全模板的名称长度为1～35字符，不区分大小写。在安全模板视图中，管理员设置了WPA2+PSK+AES安全策略，并指定密码为a1234567和b1234567。这条命令的完整语法为security { wpa | wpa2 | wpa-wap2 } psk { pass-phrase | hex } key-value { aes | tkip | aes -tkip }，在本例中，管理员选择了WPA2作为认证方式，并选择了AES作为加密方式。可以配置的密码长度为8～63字符，建议管理员在设置密码时，使用大小写字母、数字和特殊字符相结合的方式，以创建强健的密码。

（3）配置VAP模板。

VAP是虚拟AP的简称，管理员通过配置多个VAP模板，并把这些VAP模板中的配置下发到AP，就可以为移动接入设备提供具有差异化的业务。

本例中Office1和Office2办公室的无线的业务VLAN不同，认证密码也不同，因此需要创建两个VAP模板。在VAP模板中设置数据转发模式为隧道转发，指定业务VLAN，并应用之前创建的SSID模板和安全模板。

```
[AC-wlan-view]vap-profile name vap-Office1
[AC-wlan-vap-prof-vap-Office1]forward-mode tunnel
[AC-wlan-vap-prof-vap-Office1]service-vlan vlan-id 101
[AC-wlan-vap-prof-vap-Office1]ssid-profile ssid-Office1
[AC-wlan-vap-prof-vap-Office1]security-profile Sec-Office1
[AC-wlan-vap-prof-vap-Office1]quit

[AC-wlan-view]vap-profile name vap-Office2
[AC-wlan-vap-prof-vap-Office2]forward-mode tunnel
[AC-wlan-vap-prof-vap-Office2]service-vlan vlan-id 102
[AC-wlan-vap-prof-vap-Office2]ssid-profile ssid-Office2
[AC-wlan-vap-prof-vap-Office2]security-profile Sec-Office2
[AC-wlan-vap-prof-vap-Office2]quit
```

管理员在WLAN视图中使用命令vap-profile name *profile-name*，创建了名为vap-office1和vap-office2的两个VAP模板，并进入了VAP模板的配置图。VAP模板的名称长度为1～35字符，不区分大小写。

在VAP模板视图中，管理员首先通过命令forward-mode tunnel把转发模式设置为隧道转发。接着管理员使用命令service-vlan vlan-id 101指定业务VLAN为101，使用命令ssid-profile ssid-office1应用SSID模板，并使用命令security-profile sec-office1应用安全模板。

（4）在AP组中应用VAP模板。

管理员需要在AP组中应用配置好的VAP模板，这样AC才能将VAP模板的配置分发给AP，AP才能工作。AP上的射频0和射频1都使用的是VAP模板。

```
[AC-wlan-view]ap-group name ap-Office1
[AC-wlan-ap-group-ap-Office1]vap-profile vap-Office1 wlan 1 radio 0
[AC-wlan-ap-group-ap-Office1]vap-profile vap-Office1 wlan 1 radio 1
[AC-wlan-ap-group-ap-Office1]quit
[AC-wlan-view]ap-group name ap-Office2
[AC-wlan-ap-group-ap-Office2]vap-profile vap-Office2 wlan 2 radio 0
[AC-wlan-ap-group-ap-Office2]vap-profile vap-Office2 wlan 2 radio 1
[AC-wlan-ap-group-ap-Office2]quit
[AC-wlan-view]
```

管理员先使用wlan命令进入WLAN视图，然后使用命令ap-group name ap-group-office1进入AP组ap-group-office1视图。在AP组视图中，管理员使用vap-profile命令把指定的VAP模板与指定射频进行绑定。这条命令的完整语法为vap-profile *profile-name* wlan wlan-id { radio {radio-id | all } }。参数*profile-name*是之前创建的VAP模板名称；参数wlan-id是指AC中的VAP的ID，一个AC最多可以创建16个VAP，VAP ID的取值范围是1～16，本例使用了ID 1、2；参数radio-id是射频ID，本例中的AP支持射频0和射频1。其中射频0为2.4GHz射频，射频1为5GHz射频。

WLAN业务配置会由AC自动下发给AP，管理员通过命令display vap all查看AP支持的射频是否已经成功创建VAP。AP name参数显示的是管理员配置的AP名称，RfID参数表示的是射频ID，当Status参数显示为ON时，表示AP的射频ID 1已经成功创建了VAP。

```
[[AC]display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
-
AP ID AP name RfID WID  BSSID          Status        Auth type    STA
SSID
--------------------------------------------------------------------------------
-
1    ap1     0    1    00E0-FCC4-15A0 ON      WPA/WPA2-PSK  1    AP-Office1
1    ap1     1    1    00E0-FCC4-15B0 ON      WPA/WPA2-PSK  0    AP-Office1
2    ap2     0    1    00E0-FCB1-02B0 ON      WPA/WPA2-PSK  0    AP-Office1
2    ap2     1    1    00E0-FCB1-02C0 ON      WPA/WPA2-PSK  0    AP-Office1
3    ap3     0    2    00E0-FC33-5190 ON      WPA/WPA2-PSK  0    AP-Office2
3    ap3     1    2    00E0-FC33-51A0 ON      WPA/WPA2-PSK  0    AP-Office2
4    ap4     0    2    00E0-FCAF-5610 ON      WPA/WPA2-PSK  1    AP-Office2
4    ap4     1    2    00E0-FCAF-5620 ON      WPA/WPA2-PSK  0    AP-Office2
--------------------------------------------------------------------------------
-
Total: 8
```

管理员通过display vap ssid AP-Office1命令查看SSID为AP-Office1的AP支持的射频是否已经成功创建VAP。

```
[AC]display vap ssid AP-Office1
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
-
AP ID AP name RfID WID  BSSID          Status      Auth type    STA      SSID
--------------------------------------------------------------------------------
-
1    ap1    0   1    00E0-FCC4-15A0 ON      WPA/WPA2-PSK   1    AP-Office1
1    ap1    1   1    00E0-FCC4-15B0 ON      WPA/WPA2-PSK   0    AP-Office1
2    ap2    0   1    00E0-FCB1-02B0 ON      WPA/WPA2-PSK   0    AP-Office1
2    ap2    1   1    00E0-FCB1-02C0 ON      WPA/WPA2-PSK   0    AP-Office1
--------------------------------------------------------------------------------
-
Total: 4
```

输入display station all可以查看已连接的移动设备。

```
[AC]display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------
-
STA MAC  AP ID Ap name Rf/WLAN  Band  Type  Rx/Tx  RSSI  VLAN IP address
SSID
--------------------------------------------------------------------------------
-
5489-9895-16a0  1   ap1   0/1  2.4G  -  -/-  - 101  192.168.101.218   AP-
Office1
5489-98ab-4629  4   ap4   0/1  2.4G  -  -/-  - 102  192.168.102.73    AP-
Office2
--------------------------------------------------------------------------------
-
Total: 2 2.4G: 2 5G: 0
```

在上述输出信息中，STA MAC是移动设备的MAC地址，AP ID是AP的ID，AP name是AP的名称，VLAN为所属的业务VLAN，IP address为客户端获得的IP地址。可以看到有的移动设备在VLAN 101，有的移动设备在VLAN 102，并且都获得了相对应的VLAN的IP地址。

14.5　习题

1．直连式组网和旁挂式组网各有什么优势？

2．FIT AP发现AC的方式有（　　）。（多选）

A．静态发现

B．DHCP动态发现

C．FTP动态发现

D．DNS动态发现

第15章　园区网典型组网案例

本章内容

- 企业情况介绍
- 网络规划和配置

本章将介绍一个企业园区网典型组网案例。本章通过一个企业的具体的场景，介绍如何使用华为设备组建企业园区网，规划内网网段，部署有线和无线网络设备。

根据企业的需求，我们要设计高可用的企业内部网。它采用双汇聚层设计，通过VRRP实现网关冗余。在出口路由器上配置Easy IP让内网计算机通过网络地址转换访问Internet，配置NAT Server允许Internet中的计算机访问内网服务器。在出口路由器上配置ACL实现对内网计算机的上网控制。总之，本章是对HCIA认证涉及的知识和技能的一个综合运用。

15.1　企业情况介绍

15.1.1　物理拓扑

如图15-1所示，某企业有三个办公室、两个会议室和一个机房。该企业共有三个重要部门，分别为销售部、售后部、财务部，销售部有100台计算机，售后部有50台计算机，财务部有15台计算机。这三个部门的计算机在202、204、206办公室都有分布。两个会议室中使用便携式计算机和智能手机无线连接网络。机房部署了企业用到的服务器、域控制器（DC）、Web服务器和FTP服务器。

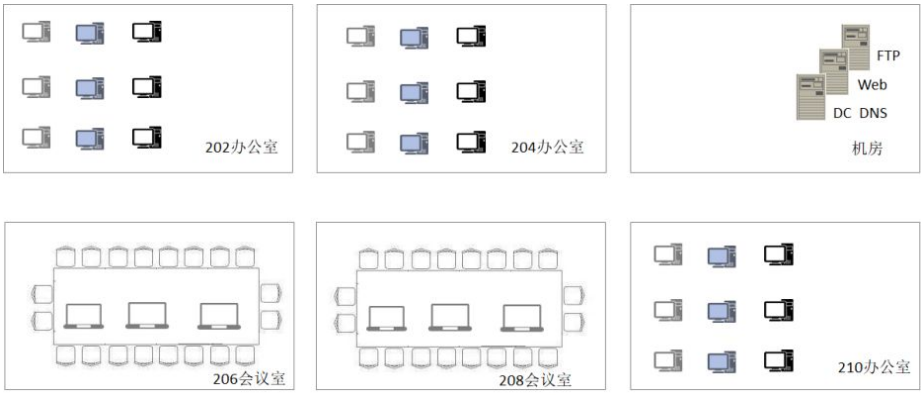


图15-1　计算机物理分布

15.1.2　组网要求

公司有线网络使用192.168.1.0/24网段，要求按部门划分VLAN；无线网络使用192.168.2.0/24网段，206会议室和208会议室无线设备要位于不同的VLAN，每个会议室最多有100台便携式计算机。

服务器要单独分配一个网段。目前有三台服务器，以后有可能增加到10台，要求从使用192.168.1.0/24网段的子网中分配一个子网。

本案例中企业对网络的要求如下。

（1）采用分层次的组网方式，即接入层、汇聚层、核心层。

（2）为企业提供Internet接入。

（3）出差员工或在家办公的员工要能够通过VPN拨入企业内网。

（4）企业Web服务器允许Internet上的用户访问。

（5）内网各个办公室的计算机和会议室的便携式计算机要能够自动获取IP地址、网关和DNS的配置。

（6）内网要求配置静态路由以实现内网各个网段的相互通信以及到Internet的访问。

（7）确保企业内网的高可用，汇聚层交换机要有冗余。

（8）汇聚层交换机之间的链路要使用链路聚合技术来实现容错和负载均衡。

（9）配置交换机使用RSTP，使得汇聚层交换机优先成为根交换机。

（10）财务部门的计算机不能访问Internet，售后部只能够访问Internet上的网站，销售部和会议室能够访问Internet，且不做任何限

制。

15.2　网络规划和配置

15.2.1　网络设备部署

从该企业的计算机物理分布和网络规模来看，组网只需二层结构就能满足要求，即在每间办公室部署一台接入层交换机，在机房部署两台汇聚层交换机和一台路由器，在208会议室部署一台AC，每间会议室部署两个AP，两个会议室的AP连接到AC。接入层交换机和AC连接，同时还连接两个汇聚层交换机。服务器连接到汇聚层交换机LSW1上，网络的物理拓扑如图15-2所示。

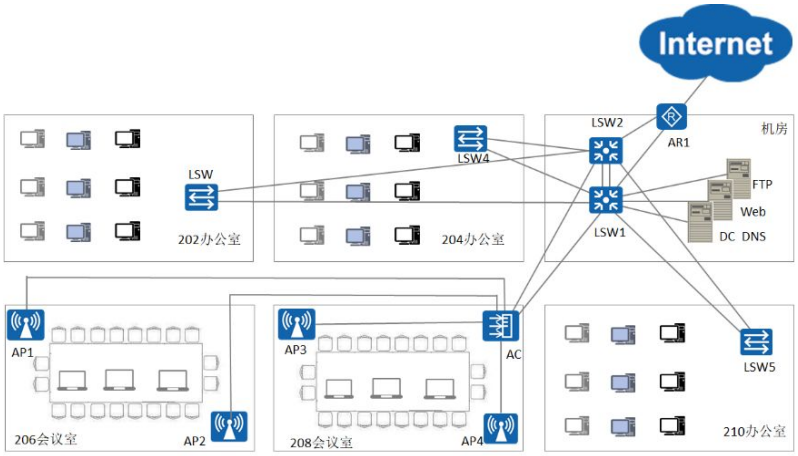


图15-2　网络物理拓扑

网络的逻辑拓扑如图15-3所示。

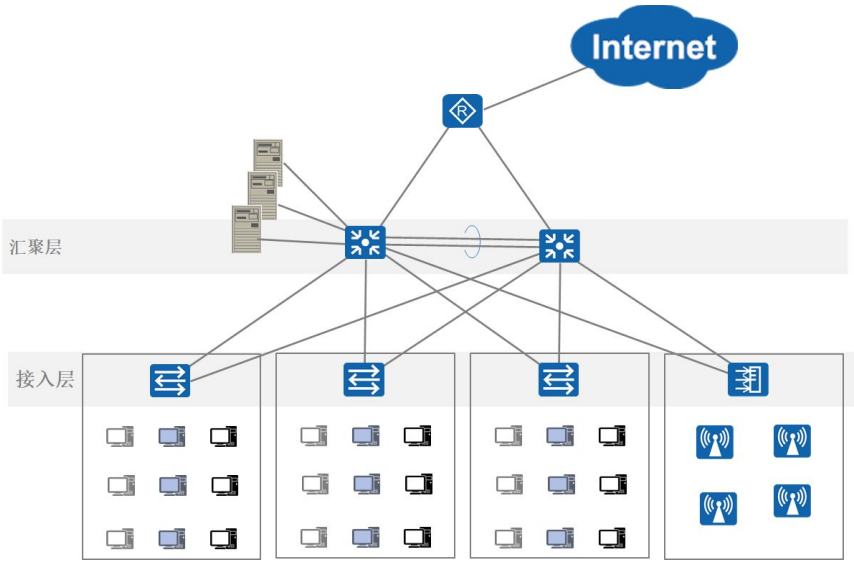


图15-3　网络逻辑拓扑

15.2.2　VLAN规划和子网划分

公司共有三个重要部门，分别为销售部、售后部、财务部，销售部有100台计算机，售后部有50台计算机，财务部有15台计算机，机房服务器要预留10个IP地址。每个部门有一个VLAN，每个VLAN要分配一个子网，并根据部门计算机数量划分子网。将192.168.1.0/24这个C类网络进行子网划分。

192.168.1.0/24网段的地址范围是192.168.1.0～192.168.1.255。将0～255用一条线段表示，如图15-4所示。该线段标出了服务器、财务部、售后部和销售部的地址分配。

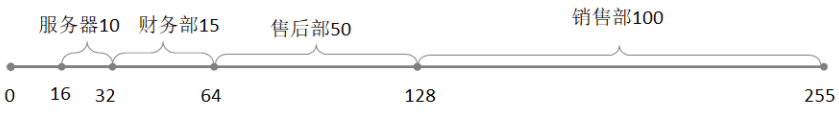


图15-4　有线网子网划分

根据图15-4为每个部门分配的地址块，写出每个子网第一个可用的IP地址和最后一个可用的IP地址，以及子网掩码。

销售部第一个可用的IP地址192.168.1.129，最后一个可用的IP地址192.168.1.254，子网掩码为255.255.255.128，销售部规划为VLAN1。

售后部第一个可用的IP地址192.168.1.65，最后一个可用的IP地址192.168.1.126，子网掩码为255.255.255.192，售后部规划为VLAN2。

财务部第一个可用的IP地址192.168.1.33，最后一个可用的IP地址192.168.1.62，子网掩码为255.255.255.224，财务部规划为VLAN3。

服务器第一个可用的IP地址192.168.1.16，最后一个可用的IP地址192.168.1.30，子网掩码为255.255.255.240，服务器规划为VLAN4。

无线网络使用192.168.2.0/24网段，该网段的地址范围为192.168.2.0～192.168.2.255。将0～255用一条线段表示，如图15-5所示。图15-5标出了206会议室的地址范围和208会议室的地址范围。

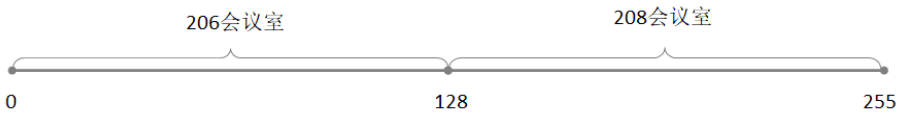


图15-5　无线网子网划分

206会议室第一个可用的IP地址192.168.2.1，最后一个可用的地址192.168.2.126，子网掩码为255.255.255.128，206会议室规划为VLAN5。

208会议室第一个可用的IP地址192.168.2.129，最后一个可用的地址192.168.2.254，子网掩码为255.255.255.128，208会议室规划为VLAN6。

15.2.3　创建VLAN配置干道链路

使用eNSP搭建本章学习环境，如图15-6所示，在LSW1、LSW2、LSW3、LSW4和LSW5上创建VLAN1～VLAN4，并且将交换机之间的连接配置成干道链路，允许VLAN1～VLAN4的帧通过。配置汇聚层交换机之间的两条链路为聚合链路，将聚合链路配置成干道，且允许所有VLAN1～VLAN4的帧通过。将服务器和每个部门的计算机指定到相应VLAN。

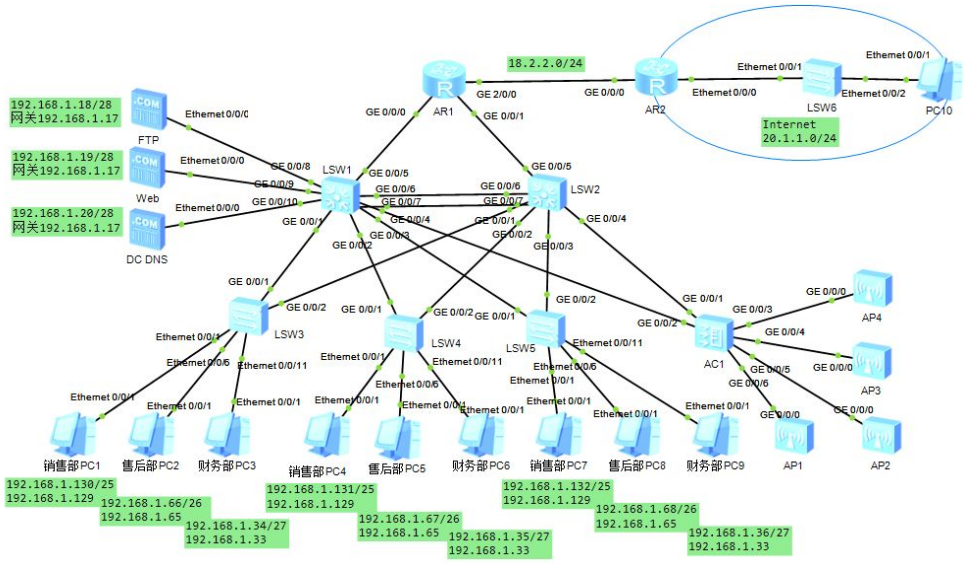


图15-6　实验环境

在LSW3上创建VLAN，将接口指定到VLAN，将GE 0/0/1和GE 0/0/2接口配置成干道链路。

```
<Huawei>sys
[Huawei]sysname LSW3
[LSW3]vlan batch 2 3 4
[LSW3]port-group vlan1port
[LSW3-port-group-vlan1port]
[LSW3-port-group-vlan1port]group-member Ethernet 0/0/1 to Ethernet
0/0/5
[LSW3-port-group-vlan1port]port link-type access
[LSW3-port-group-vlan1port]port default vlan 1
[LSW3-port-group-vlan1port]quit
[LSW3]port-group vlan2port
[LSW3-port-group-vlan2port]
[LSW3-port-group-vlan2port]group-member Ethernet 0/0/6 to Ethernet
0/0/10
[LSW3-Ethernet0/0/10]port link-type access
[LSW3-port-group-vlan2port]port default vlan 2
[LSW3-port-group-vlan2port]quit
[LSW3]port-group vlan3port
[LSW3-port-group-vlan3port]group-member Ethernet 0/0/11 Ethernet
0/0/15
[LSW3-port-group-vlan3port]port link-type access
[LSW3-port-group-vlan3port]port default vlan 3
[LSW3-port-group-vlan3port]quit
[LSW3]port-group trunkport
[LSW3-port-group-trunkport]group-member GigabitEthernet 0/0/1 to
GigabitEthernet 0/0/2
[LSW3-port-group-trunkport]port link-type trunk
[LSW3-port-group-trunkport]port trunk allow-pass vlan 1 2 3 4
[LSW3-port-group-trunkport]quit
```

在LSW4和LSW5上的配置类似，这里不再赘述。

在LSW1上的配置如下，创建VLAN，配置干道接口，再配置聚合链路。

```
[Huawei]sysname LSW1
[LSW1]vlan batch 2 3 4
[LSW1]port-group vlan4port
[LSW1-port-group-vlan4port]group-member GigabitEthernet 0/0/8
GigabitEthernet 0/0/10
[LSW1-port-group-vlan4port]port link-type access
[LSW1-port-group-vlan4port]port default vlan 4
[LSW1-port-group-vlan4port]quit
[LSW1]port-group trunkport
[LSW1-port-group-trunkport]group-member GigabitEthernet 0/0/1 to
GigabitEthernet 0/0/3
[LSW1-port-group-trunkport]port link-type trunk
```

```
[LSW1-port-group-trunkport]port trunk allow-pass vlan 1 2 3 4
[LSW1-port-group-trunkport]quit

[LSW1]interface Eth-Trunk 1
[LSW1-Eth-Trunk1]mode manual load-balance
[LSW1-Eth-Trunk1]trunkport GigabitEthernet 0/0/6 to 0/0/7
[LSW1-Eth-Trunk1]port link-type trunk
[LSW1-Eth-Trunk1]port trunk allow-pass vlan 1 2 3 4
[LSW1-Eth-Trunk1]quit
```

在LSW2上的配置如下，创建VLAN，配置干道接口，再配置聚合链路。

```
[Huawei]sysname LSW2
[LSW2]vlan batch 2 3 4
[LSW2]port-group trunkport
[LSW2-port-group-trunkport]group-member GigabitEthernet 0/0/1 to
GigabitEthernet 0/0/3
[LSW2-port-group-trunkport]port link-type trunk
[LSW2-port-group-trunkport]port trunk allow-pass vlan  1 2 3 4
[LSW2-port-group-trunkport]quit
[LSW2]interface Eth-Trunk 1
[LSW2-Eth-Trunk1]mode manual load-balance
[LSW2-Eth-Trunk1]trunkport GigabitEthernet 0/0/6 to 0/0/7
[LSW2-Eth-Trunk1]port link-type trunk
[LSW2-Eth-Trunk1]port trunk allow-pass vlan 1 2 3 4
[LSW2-Eth-Trunk1]quit
```

15.2.4　指定生成树的根交换机

配置网络中的交换机使用RSTP，在本例中，将汇聚层交换机LSW1指定为根交换机，LSW2指定为备用根交换机。

```
[LSW1]stp mode rstp
[LSW1]stp priority 0
[LSW2]stp mode rstp
[LSW2]stp priority 4096
[LSW3]stp mode rstp
[LSW4]stp mode rstp
[LSW5]stp mode rstp
```

15.2.5　配置VLAN间路由

在将汇聚层交换机和接入层交换机之间的连接配置成干道链路后，在LSW1和LSW2上实现VLAN间路由，图15-7为等价的逻辑图。可以将LSW1和LSW2看作路由器，每个VLAN有两个路由器，使用VRRP将Virtual ip配置为VLAN中第一个可用的地址，LSW1交换机的vlanif接口的地址为各个VLAN的倒数第二个可用地址，LSW2交换机的vlanif接口的地址为各个VLAN的倒数第一个可用地址。

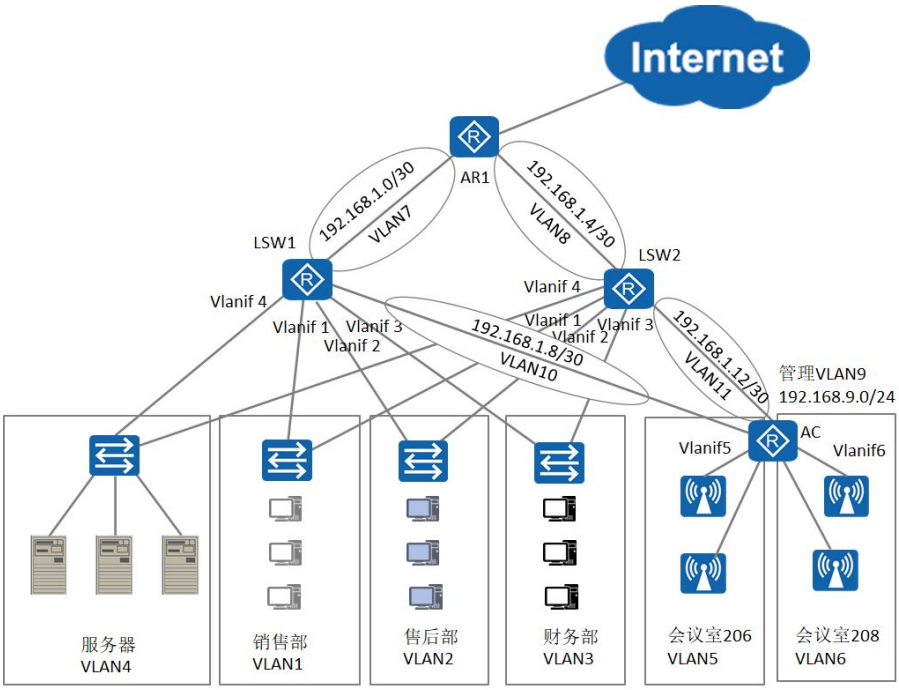


图15-7　无线网络连接有线网络

LSW1和AR1之间的连接需要一个独立的网段，在LSW1上创建VLAN7以和AR1连接，使用192.168.1.0/30网段。LSW2和AR1之间的连接也需要一个独立的网段，在LSW2上创建VLAN8以和AR1连接，使用192.168.1.4/30网段。AC可看作一个路由器，通过VLAN10来与LSW1连接，使用

192.168.1.8/30网段；AC和LSW2的连接通过VLAN11，使用192.168.1.12/30网段。

VLAN 1、2、3、4的网关优先由LSW1上的VRRP虚拟网关优先在LSW1上，VRRP的优先级根据连接路由器的vlanif接口进行调整。无线网络访问Internet优先走LSW2，当LSW2出现故障时，无线网络访问Internet走LSW1。

在LSW1上配置接口地址。

```
[LSW1]interface Vlanif 1
[LSW1-Vlanif1]ip address 192.168.1.253 25
[LSW1-Vlanif1]quit
[LSW1]interface Vlanif 2
[LSW1-Vlanif2]ip address 192.168.1.125 26
[LSW1-Vlanif2]quit
[LSW1]interface Vlanif 3
[LSW1-Vlanif3]ip address 192.168.1.61 27
[LSW1-Vlanif3]quit
[LSW1]interface Vlanif 4
[LSW1-Vlanif4]ip address 192.168.1.17 28
[LSW1-Vlanif4]quit
```

在LSW2上配置接口地址。

```
[LSW2]interface Vlanif 1
[LSW2-Vlanif1]ip address 192.168.1.254 25
[LSW2-Vlanif1]quit
[LSW2]interface Vlanif 2
[LSW2-Vlanif2]ip address 192.168.1.126 26
[LSW2-Vlanif2]quit
[LSW2]interface Vlanif 3
[LSW2-Vlanif4]interface Vlanif 3
[LSW2-Vlanif3]ip address 192.168.1.62 27
[LSW2-Vlanif3]quit
[LSW2]interface Vlanif 4
[LSW2-Vlanif4]ip address 192.168.1.30 28
[LSW2-Vlanif4]quit
```

在LSW1上创建VLAN 7，将GE 0/0/5接口加入VLAN 7，配置vlanif 7的IP地址。在LSW2上创建VLAN 8，将GE 0/0/5接口加入VLAN 8，配置vlanif 8的IP地址。

```
[LSW1]vlan 7
[LSW1-vlan7]quit
[LSW1]interface GigabitEthernet 0/0/5
[LSW1-GigabitEthernet0/0/5]port link-type access
[LSW1-GigabitEthernet0/0/5]port default vlan 7
[LSW1-GigabitEthernet0/0/5]quit
[LSW1]interface Vlanif 7
[LSW1-Vlanif7]ip address 192.168.1.1 30

[LSW2]vlan 8
[LSW2-vlan8]quit
[LSW2]interface GigabitEthernet 0/0/5
[LSW2-GigabitEthernet0/0/5]port link-type access
[LSW2-GigabitEthernet0/0/5]port default vlan 8
[LSW2-GigabitEthernet0/0/5]quit
[LSW2]interface Vlanif 8
[LSW2-Vlanif8]ip address 192.168.1.5 30
```

在LSW1上配置VRRP，将每个VLAN的第一个地址作为虚拟网关地址。

```
[LSW1]interface Vlanif 1
[LSW1-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.129
[LSW1-Vlanif1]vrrp vrid 1 priority 120
[LSW1-Vlanif1]vrrp vrid 1 track interface Vlanif 7 reduced 40
[LSW1-Vlanif1]vrrp vrid 1 preempt-mode timer delay 10

[LSW1]interface Vlanif 2
[LSW1-Vlanif2]vrrp vrid 1 virtual-ip 192.168.1.65
[LSW1-Vlanif2]vrrp vrid 1 priority 120
[LSW1-Vlanif2]vrrp vrid 1 track interface Vlanif 7 reduced 40
[LSW1-Vlanif2]vrrp vrid 1 preempt-mode timer delay 10

[LSW1]interface Vlanif 3
[LSW1-Vlanif3]vrrp vrid 1 virtual-ip 192.168.1.33
[LSW1-Vlanif3]vrrp vrid 1 priority 120
[LSW1-Vlanif3]vrrp vrid 1 track interface Vlanif 7 reduced 40
[LSW1-Vlanif3]vrrp vrid 1 preempt-mode timer delay 10
```

在LSW2上配置VRRP，将VLAN的第一个地址作为虚拟网关地址。

```
[LSW2]interface Vlanif 1
[LSW2-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.129
[LSW2]interface Vlanif 2
[LSW2-Vlanif2]vrrp vrid 1 virtual-ip 192.168.1.65
[LSW2]interface Vlanif 3
[LSW2-Vlanif3]vrrp vrid 1 virtual-ip 192.168.1.33
```

查看VRRP的摘要信息。可以看到LSW2的Vlanif1、Vlanif2、Vlanif3接口的状态是Backup。

```
<LSW2>display vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------------------
1     Backup       Vlanif1                  Normal   192.168.1.129
1     Backup       Vlanif2                  Normal   192.168.1.65
1     Backup       Vlanif3                  Normal   192.168.1.33
------------------------------------------------------------------------------
Total:3    Master:0     Backup:3     Non-active:0
```

15.2.6 配置静态路由

LSW1和AR1之间的连接使用192.168.1.0/30网段的地址，LSW2和AR1之间的连接使用192.168.1.4/30网段的地址。在两个汇聚层交换机上添加默认路由以指向AR1路由器。

在LSW1上创建VLAN7，配置Vlanif 7接口，添加默认路由指向AR1路由器。

```
[LSW1]vlan 7
[LSW1-vlan7]quit
[LSW1]interface GigabitEthernet 0/0/5
[LSW1-GigabitEthernet0/0/5]port link-type access
[LSW1-GigabitEthernet0/0/5]port default vlan 7
[LSW1-GigabitEthernet0/0/5]quit
[LSW1]interface Vlanif7
[LSW1-Vlanif7]ip address 192.168.1.1 30
[LSW1-Vlanif7]quit
[LSW1]ip route-static 0.0.0.0 0 192.168.1.2
```

在LSW2上创建VLAN8，配置Vlanif 8接口，添加默认路由指向AR1路由器。

```
[LSW2]vlan 8
[LSW2-vlan8]quit
[LSW2]interface GigabitEthernet 0/0/5
[LSW2-GigabitEthernet0/0/5]port link-type access
[LSW2-GigabitEthernet0/0/5]port default vlan 8
[LSW2-GigabitEthernet0/0/5]quit
[LSW2]interface Vlanif8
[LSW2-Vlanif8]ip address 192.168.1.5 30
[LSW2-Vlanif8]quit
[LSW2]ip route-static 0.0.0.0 0 192.168.1.6
```

在AR1路由器上配置接口IP地址。添加一条默认路由，它指向Internet的路由器AR2，然后添加浮动静态路由。到内网的VLAN1、VLAN2、VLAN3和VLAN4网段的数据包优先转发给LSW1，到无线网络的数据包优先转发给LSW2。

```
[Huawei]sysname AR1
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ip address 192.168.1.2 30
[AR1-GigabitEthernet0/0/0]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]ip address 192.168.1.6 30
[AR1-GigabitEthernet0/0/1]interface GigabitEthernet 2/0/0
[AR1-GigabitEthernet2/0/0]ip address 18.2.2.1 24
[AR1-GigabitEthernet2/0/0]quit
[AR1]ip route-static 0.0.0.0 0 18.2.2.2
[AR1]ip route-static 192.168.1.0 255.255.255.0 192.168.1.1
preference 40
[AR1]ip route-static 192.168.1.0 255.255.255.0 192.168.1.5
preference 60
[AR1]ip route-static 192.168.2.0 255.255.255.0 192.168.1.1
preference 60
[AR1]ip route-static 192.168.2.0 255.255.255.0 192.168.1.5
preference 40
```

15.2.7　将汇聚层交换机配置成DHCP

本案例将汇聚层交换机LSW1配置成VLAN1、VLAN2、VLAN3的DHCP服务器。不能在LSW2上创建这三个VLAN的DHCP地址池。VRRP的Virtual ip在哪个交换机上就在那个交换机上配置该网段的DHCP地址池。这种情况一定要配置接口从全局获得IP地址，客户端才能获得正确的网关。

```
[LSW1]dhcp enable
[LSW1]ip pool vlan1
[LSW1-ip-pool-vlan1]network 192.168.1.128 mask 25
[LSW1-ip-pool-vlan1]gateway-list 192.168.1.129
[LSW1-ip-pool-vlan1]dns-list 192.168.1.20
[LSW1-ip-pool-vlan1]lease day 0 hour 8 minute 0
[LSW1-ip-pool-vlan1]excluded-ip-address 192.168.1.253 192.168.1.254
[LSW1-ip-pool-vlan1]quit
[LSW1]interface Vlanif 1
[LSW1-Vlanif1]dhcp select global

[LSW1]ip pool vlan2
[LSW1-ip-pool-vlan2]network 192.168.1.64 mask 26
[LSW1-ip-pool-vlan2]gateway-list 192.168.1.65
[LSW1-ip-pool-vlan2]dns-list 192.168.1.20
[LSW1-ip-pool-vlan2]lease day 0 hour 8 minute 0
[LSW1-ip-pool-vlan2]excluded-ip-address 192.168.1.125 192.168.1.126
[LSW1-ip-pool-vlan2]quit
[LSW1]interface Vlanif 2
[LSW1-Vlanif2]dhcp select global

[LSW1]ip pool vlan3
[LSW1-ip-pool-vlan3]network 192.168.1.32 mask 27
[LSW1-ip-pool-vlan3]gateway-list 192.168.1.33
[LSW1-ip-pool-vlan3]dns-list 192.168.1.20
[LSW1-ip-pool-vlan3]lease day 0 hour 8 minute 0
[LSW1-ip-pool-vlan3]excluded-ip-address 192.168.1.61 192.168.1.62
[LSW1-ip-pool-vlan3]quit
[LSW1]interface Vlanif 3
[LSW1-Vlanif3]dhcp select global
```

15.2.8　配置WLAN

在本例中，会议室206和208分别规划为VLAN5和VLAN6，分配的网段分别为192.168. 2.0/25和192.168.2.128/25。VLAN间的路由在AC上实

现，这时可以把AC看成一台路由器，逻辑图如图15-8所示。

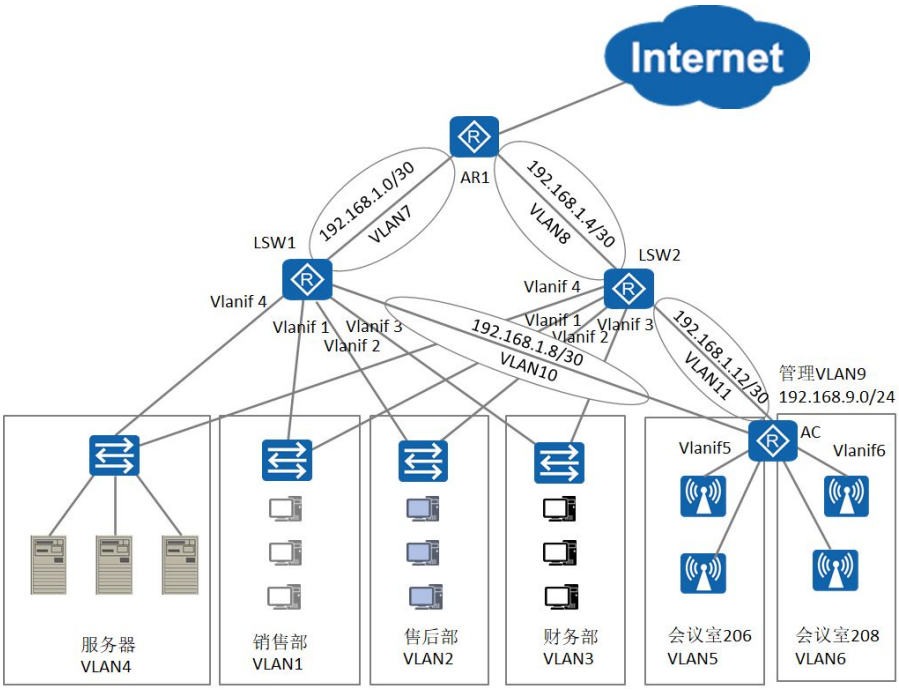


图15-8　无线网

AC和AP之间的管理VLAN使用VLAN9，分配的网段为192.168.9.0/24。

在AC上的配置如下，创建VLAN。

```
[AC]vlan batch 5 6 9 10 11
```

配置VLAN接口地址，启用DHCP，为AP分配地址，然后为无线设备分配地址。

```
[AC]dhcp enable
[AC]interface Vlanif 9
[AC-Vlanif9]ip address 192.168.9.1 24
[AC-Vlanif9]dhcp select interface
[AC]interface Vlanif 5
[AC-Vlanif5]ip address 192.168.2.1 25
```

```
[AC-Vlanif5]dhcp select interface
[AC-Vlanif5]quit
[AC]interface Vlanif 6
[AC-Vlanif6]ip address 192.168.2.129 25
[AC-Vlanif6]dhcp select interface
[AC-Vlanif6]quit
```

配置管理VLAN。

```
[AC]port-group ap-port
[AC-port-group-ap-port]group-member GigabitEthernet 0/0/3 to
GigabitEthernet 0/0/6
[AC-port-group-ap-port]port link-type trunk
[AC-port-group-ap-port]port trunk pvid vlan 9
[AC-port-group-ap-port]port trunk allow-pass vlan 9
```

设置AC的源接口，AC使用Vlanif 9接口的地址作为源地址与AP进行通信。

```
[AC]capwap source interface Vlanif 9
```

配置域管理模板，设置国家码。

```
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name domain-cn
[AC-wlan-regulate-domain-domain-cn]country-code cn
[AC-wlan-regulate-domain-domain-cn]quit
```

创建AP组，指定域管理模板。

```
[AC-wlan-view]ap-group name ap-group-206
[AC-wlan-ap-group-ap-group-206]regulatory-domain-profile domain-cn
Warning: Modifying the country code will clear channel, power and
antenna gain configurations of the radio and reset the AP. Continue?
[Y/N]:y
[AC-wlan-ap-group-ap-group-206]quit
[AC-wlan-view]ap-group name ap-group-208
[AC-wlan-ap-group-ap-group-208]regulatory-domain-profile domain-cn
Warning: Modifying the country code will clear channel, power and
antenna gain configurations of the radio and reset the AP. Continue?
[Y/N]:y
```

```
[AC-wlan-ap-group-ap-group-208]quit
[AC-wlan-view]
```

在AC上以MAC地址认证的方式添加AP。

```
[AC-wlan-view]ap-id 1 ap-mac 00E0-FC94-25B0
[AC-wlan-ap-1]ap-group ap-group-206
Warning: This operation may cause AP reset. If the country code
changes, it will
clear channel, power and antenna gain configurations of the radio,
Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a
moment.. done.
[AC-wlan-ap-1]quit
[AC-wlan-view]ap-id 2 ap-mac 00E0-FCAF-7440
[AC-wlan-ap-2]ap-group ap-group-206
Warning: This operation may cause AP reset. If the country code
changes, it will
 clear channel, power and antenna gain configurations of the radio,
Whether to c
ontinue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a
moment.. done.
[AC-wlan-ap-2]quit
[AC-wlan-view]ap-id 3 ap-mac 00E0-FCCB-6E10
[AC-wlan-ap-3]ap-name ap3
[AC-wlan-ap-3]ap-group ap-group-208
Warning: This operation may cause AP reset. If the country code
changes, it will
 clear channel, power and antenna gain configurations of the radio,
Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a
moment.. done.
[AC-wlan-ap-3]quit
[AC-wlan-view]ap-id 4 ap-mac 00E0-FCB7-66F0
[AC-wlan-ap-4]ap-name ap4
[AC-wlan-ap-4]ap-group ap-group-208
Warning: This operation may cause AP reset. If the country code
changes, it will
 clear channel, power and antenna gain configurations of the radio,
Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a
moment.. done.
[AC-wlan-ap-4]quit
```

配置SSID模板，为每一间办公室指定一个SSID。

```
[AC]wlan
[AC-wlan-view]ssid-profile name ssid-206
[AC-wlan-ssid-prof-ssid-206]ssid 206-AP
[AC-wlan-ssid-prof-ssid-206]quit
[AC-wlan-view]ssid-profile name ssid-208
[AC-wlan-ssid-prof-ssid-208]ssid 208-AP
[AC-wlan-ssid-prof-ssid-208]quit
[AC-wlan-view]
```

配置安全模板，指定无线AP连接的密码和认证方式。

```
[AC]wlan
[AC-wlan-view]security-profile name sec-206
[AC-wlan-sec-prof-sec-206]security wpa2 psk pass-phrase 91xueit.com
aes
[AC-wlan-sec-prof-sec-206]quit
[AC-wlan-view]security-profile name sec-208
[AC-wlan-sec-prof-sec-208]security wpa2 psk pass-phrase 51cto.com
aes
[AC-wlan-sec-prof-sec-208]quit
[AC-wlan-view]
```

配置VAP模板，指定连接会议室的AP的设备所属的VLAN、使用的安全模板以及SSID。

```
[AC-wlan-view]vap-profile name vap-206
[AC-wlan-vap-prof-vap-206]forward-mode tunnel
[AC-wlan-vap-prof-vap-206]service-vlan vlan-id 5
[AC-wlan-vap-prof-vap-206]ssid-profile ssid-206
[AC-wlan-vap-prof-vap-206]security-profile sec-206
[AC-wlan-vap-prof-vap-206]quit

[AC-wlan-view]vap-profile name vap-208
[AC-wlan-vap-prof-vap-208]forward-mode tunnel
[AC-wlan-vap-prof-vap-208]service-vlan vlan-id 6
[AC-wlan-vap-prof-vap-208]ssid-profile ssid-208
[AC-wlan-vap-prof-vap-208]security-profile sec-208
[AC-wlan-vap-prof-vap-208]quit
[AC-wlan-view]
```

在AP组中应用VAP模板，在AP应用后开始工作。

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group-206
```

```
[AC-wlan-ap-group-ap-group-206]vap-profile vap-206 wlan 1 radio 0
[AC-wlan-ap-group-ap-group-206]quit
[AC-wlan-view]ap-group name ap-group-208
[AC-wlan-ap-group-ap-group-208]vap-profile vap-208 wlan 2 radio 1
[AC-wlan-ap-group-ap-group-208]quit
[AC-wlan-view]quit
```

15.2.9 配置到WLAN网络的路由

无线网络访问Internet时优先通过LSW2进行，当LSW2出现故障后，无线网络访问Internet时通过LSW1进行。

在LSW1上创建VLAN 10，配置Vlanif 10接口地址和AC连接，然后添加到无线网络的路由。

```
[LSW1]vlan 10
[LSW1-vlan10]quit
[LSW1]interface GigabitEthernet 0/0/4
[LSW1-GigabitEthernet0/0/4]port link-type access
[LSW1-GigabitEthernet0/0/4]port default vlan 10
[LSW1-GigabitEthernet0/0/4]quit
[LSW1]interface Vlanif 10
[LSW1-Vlanif10]ip address 192.168.1.10 30
[LSW1-Vlanif10]quit
[LSW1]ip route-static 192.168.2.0 255.255.255.0 192.168.1.9
```

在LSW2上创建VLAN 11，配置Vlanif 11接口地址和AC连接，然后添加到无线网络的路由。

```
[LSW2]vlan 11
[LSW2-vlan11]quit
[LSW2]interface GigabitEthernet 0/0/4
[LSW2-GigabitEthernet0/0/4]port link-type access
[LSW2-GigabitEthernet0/0/4]port default vlan 11
[LSW2-GigabitEthernet0/0/4]quit
[LSW2]interface Vlanif 11
[LSW2-Vlanif11]ip address 192.168.1.14 30
[LSW2-Vlanif11]quit
[LSW2]ip route-static 192.168.2.0 255.255.255.0 192.168.1.13
[LSW2]
```

在AC上将GigabitEthernet 0/0/2接口添加到VLAN10，将GigabitEthernet 0/0/1接口添加到VLAN11。给Vlanif 10接口、Vlanif 11接口配置IP地址和子网掩码。添加两条默认路由，指定不同优先级，优先转发到LSW2。

```
[AC]interface GigabitEthernet 0/0/2
[AC-GigabitEthernet0/0/2]port link-type access
[AC-GigabitEthernet0/0/2]port default vlan 10
[AC-GigabitEthernet0/0/2]quit
[AC]interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1]port link-type access
[AC-GigabitEthernet0/0/1]port default vlan 11
[AC-GigabitEthernet0/0/1]quit
[AC]interface Vlanif 10
[AC-Vlanif10]ip address 192.168.1.9 30
[AC-Vlanif10]quit
[AC]interface Vlanif 11
[AC-Vlanif11]ip address 192.168.1.13 30
[AC-Vlanif11]quit

[AC]ip route-static 0.0.0.0 0 192.168.1.10 preference 60
[AC]ip route-static 0.0.0.0 0 192.168.1.14 preference 40
```

15.2.10 配置网络地址转换和端口映射

在本例中，AR1路由器只有一个公网地址，让内网计算机通过AR1的GE 2/0/0接口的公网地址访问Internet。

```
[AR1]acl 2000
[AR1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[AR1-acl-basic-2000]rule 10 permit source 192.168.2.0 0.0.0.255
[AR1-acl-basic-2000]rule 15 deny
[AR1-acl-basic-2000]quit
[AR1]interface GigabitEthernet 2/0/0
[AR1-GigabitEthernet2/0/0]nat outbound 2000
```

在AR1路由器上配置端口映射，允许Internet上的计算机访问内网网站。

```
[AR1-GigabitEthernet2/0/0]nat server protocol tcp global current-
interface www inside 192.168.1.19 www
```

15.2.11　创建ACL实现内网上网控制

在本例中，销售部、会议室206、会议室208允许使用任何协议访问Internet，售后部只允许访问Internet上的网站，且允许使用ping命令测试到Internet的连通性，财务部不允许访问Internet。

允许访问Internet网站，就需要允许域名解析，DNS协议使用UDP的53端口，HTTP使用TCP的80端口，有些网站使用HTTPS访问，HTTPS使用TCP的443端口，ping命令使用的是ICMP。最后别忘了内网Web服务器允许Internet用户访问。

如图15-9所示，ACL被设置在AR1路由器上，绑定到接口GE 0/0/0和GE 0/0/1的入站方向。为什么不将ACL绑定到AR1接口的GE2/0/0出站方向呢？因为在AR1上配置网络地址转换，内网的计算机访问Internet的数据包，先进行网络地址转换，源地址被替换成公网地址了，就不能根据源地址进行数据包过滤了。

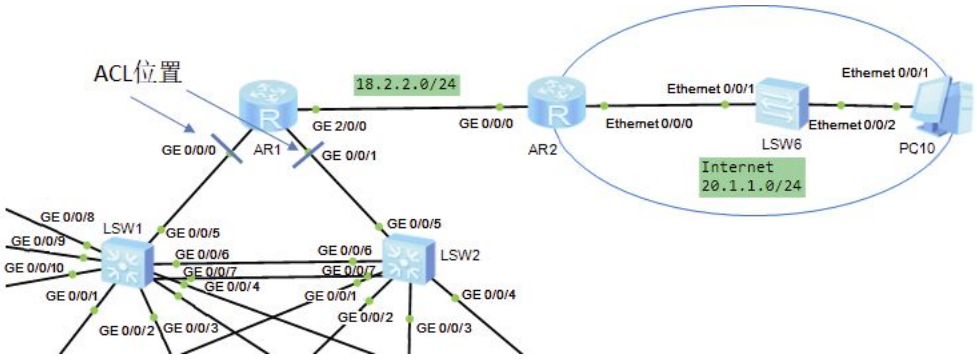


图15-9　ACL的位置和方向

```
[AR1]acl 3000
[AR1-acl-adv-3000]rule 5 permit ip source 192.168.1.128 0.0.0.127
[AR1-acl-adv-3000]rule 10 permit ip source 192.168.2.0 0.0.0.255
[AR1-acl-adv-3000]rule 15 permit tcp source 192.168.1.64 0.0.0.191
destination-port eq 80
[AR1-acl-adv-3000]rule 20 permit tcp source 192.168.1.64 0.0.0.191
destination-port eq 443
[AR1-acl-adv-3000]rule 25 permit udp source 192.168.1.64 0.0.0.191
destination-port eq 53
[AR1-acl-adv-3000]rule 30 permit icmp source 192.168.1.64 0.0.0.191
[AR1-acl-adv-3000]rule 35 permit ip source 192.168.1.19 0.0.0.0
[AR1-acl-adv-3000]rule 40 deny ip
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]traffic-filter inbound acl 3000
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]traffic-filter inbound acl 3000
[AR1-GigabitEthernet0/0/1]quit
```

15.2.12 配置VPN

该企业允许员工在企业之外的地方访问企业内网，因此需要将AR1配置成远程访问服务器。

在本案例中，给远程拨入计算机分配192.168.3.0/24网段的地址。

创建VPN拨入用户。

```
[AR1]aaa
[AR1-aaa]local-user hanligang password cipher 91xueit
[AR1-aaa]local-user hanlgiang service-type ppp
[AR1-aaa]quit
```

为远程拨入计算机创建地址池。

```
[AR1]ip pool remotePool
[AR1-ip-pool-remotePool]network 192.168.3.0 mask 24
[AR1-ip-pool-remotePool]gateway-list 192.168.3.1
[AR1-ip-pool-remotePool]quit
```

创建虚拟模板。

```
[AR1]interface Virtual-Template 1
[AR1-Virtual-Template1]ip address 192.168.3.1 24
[AR1-Virtual-Template1]ppp  authentication-mode pap
[AR1-Virtual-Template1]remote address pool remotePool
[AR1-Virtual-Template1]quit
```

启用L2TP，配置L2TP组，启用隧道身份验证，指定隧道密码和使用的模板。

```
[AR1]l2tp enable
[AR1]l2tp-group 1
[AR1-l2tp1]tunnel authentication
[AR1-l2tp1]tunnel password simple huawei
[AR1-l2tp1]allow l2tp virtual-template 1
[AR1-l2tp1]quit
```

VPN拨通之后只能够访问销售部和售后部，不能够ping通财务部和服务器VLAN4。如果想让VPN用户访问内网全部网段，则需要在ACL 3000中添加几条规则。

```
[AR1-acl-adv-3000]rule 28 permit ip source 192.168.1.0 0.0.0.255
destination 192.168.3.0 0.0.0.255
[AR1-acl-adv-3000]rule 29 permit ip source 192.168.2.0 0.0.0.255
destination 192.168.3.0 0.0.0.255
```